PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-196624

(43)Date of publication of application : 11.07.2003

(51)Int.Cl. G06K 19/07
B42D 15/10
G06F 3/08
G06K 19/073

(21)Application number : 2001-397292

(22)Date of filing : 27.12.2001

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

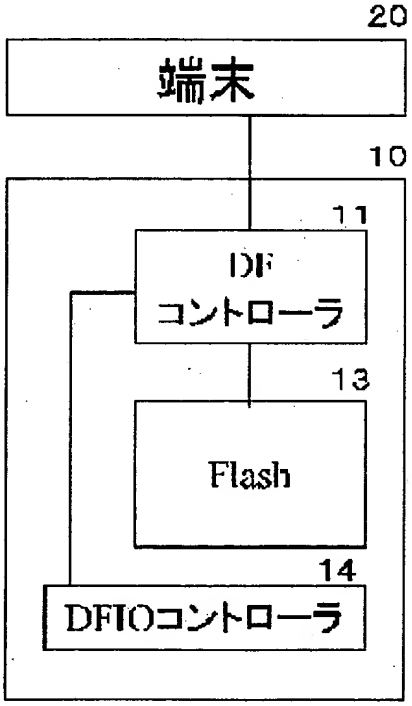
(72)Inventor : SASAKI OSAMU
NAKANISHI YOSHIAKI
TAKAGI YOSHIHIKO

(54) DUAL FUNCTION CARD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a DF (dual function) card eliminating any room for intervening a fraudulent action by a terminal, preventing fraudulent writing/reading of data from the outside, and retaining the secrecy and the completeness of the stored data.

SOLUTION: This DF card 10 incorporating a terminal communication interface with the terminal 20, an external communication interface with the outside, and data storage means 13 is provided with a command execution means 11 executing a command received from the terminal, a storage control means 11 receiving the command of the command execution means and controlling the writing reading of transmission data from the external communication interface, and an external communication control means 14 for receiving the command of the command execution means and controlling the input output of the communication data from the external communication interface. Under the command of the terminal, this DF card outputs internal data to the outside without intervention of the terminal and storing the external data without intervention of the terminal so a to prevent the fraudulent action by the terminal and retain the secrecy and the completeness of the internal data of the card.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] A terminal communication interface with a terminal, and an external communication interface with the exterior, An instruction-execution means to be the dual function card which contains a data storage means, and to execute the instruction received from said terminal communication interface or the external communication interface, A storage control means to control writing and read-out of data for said storage means in response to the instruction of said instruction-execution means, The dual function card characterized by having an external communications control means to control I/O of the commo data from said external communication interface in response to the instruction of said instruction-execution means.
[Claim 2] The dual function card according to claim 1 characterized by said storage control means and an external communications control means operating only in response to the instruction of said instruction-execution means.
[Claim 3] The dual function card according to claim 1 with which said instruction-execution means and a storage control means are characterized by being mounted as software on a tamper-proof IC chip.
[Claim 4] The dual function card according to claim 3 with which said external communications control means is characterized by being mounted as software on a tamper-proof IC chip with said instruction-execution means and the storage control means.
[Claim 5] The dual function card according to claim 1 characterized by mounting said instruction-execution means as software on a tamper-proof IC chip, and mounting respectively said storage control means and the external communications control means as hardware of tamper-proof nature.
[Claim 6] The dual function card according to claim 1 characterized by said instruction-execution means outputting the data read from said storage means through said storage control means from said external communication interface through said external communications control means.
[Claim 7] Said instruction-execution means is a dual function card according to claim 1 characterized by to perform actuation which reads data from said storage means through said storage control means, and actuation which outputs said data from said external communication interface through said external communications control means in response to the instruction which outputs outside the data stored with said storage means from a terminal, without minding a terminal.
[Claim 8] The dual function card according to claim 1 with which said instruction-execution means is characterized by showing a terminal the contents of the data inputted from said external communication interface.
[Claim 9] Said instruction-execution means is a dual function card according to claim 8 characterized by creating the contents presentation data showing the contents of said data, and showing a terminal said contents presentation data.
[Claim 10] Said instruction-execution means is a dual function card according to claim 8 or 9 characterized by storing in said storage means said data inputted from said external communication interface through said storage control means in response to directions of said terminal.
[Claim 11] When data input said instruction-execution means from said external communication interface, The actuation which creates the contents presentation data showing the contents of said data, and is shown to a terminal, The dual function card according to claim 1 characterized by performing actuation which stores said data in said storage means through said storage control means from a terminal in response to the instruction which stores in said storage means the data received by said external communication interface, without minding a terminal.
[Claim 12] The dual function card according to claim 1 characterized by for said instruction-execution means creating the contents presentation data showing the contents of the data read from said storage means through said storage control means, and showing a terminal.
[Claim 13] Said instruction-execution means is a dual function card according to claim 12 characterized by creating the contents presentation data showing the contents of the corresponding data, and showing a terminal when there is a demand of data from the exterior through said external communication interface.
[Claim 14] Said instruction-execution means is a dual function card according to claim 13 characterized by outputting said data from said external communication interface through said external communications control means in response to directions of said terminal.
[Claim 15] The dual function card according to claim 6 or 14 characterized by said instruction-execution means enciphering said data outputted through said external communications control means.
[Claim 16] When a data demand inputs said instruction-execution means from said external communication interface, The actuation which reads the demanded data from said storage means through said storage control means, The actuation which creates the contents presentation data showing the contents of said data, and is shown to a terminal, From a terminal, the data stored in said storage means in response to the external data demand The dual function card according to claim 1 characterized by performing actuation which outputs said data from said external communication interface through said external communications control means in response to the instruction outputted outside, without minding a terminal.
[Claim 17] Not storing in said storage means the data into which said instruction-execution means or a storage means is inputted from said terminal communication interface, or/and the data read from said storage means are a dual function card according to claim 1 which sends out and twists to said terminal communication interface, and is characterized by things.
[Claim 18] The instruction which is an instruction taken out from a terminal to the dual function card which contains a terminal

communication interface, an external communication interface with the exterior, and a data storage means with a terminal, and directs to output outside the data held with said storage means, without minding a terminal.
[Claim 19] The instruction which is an instruction taken out from a terminal to the dual function card which contains a terminal communication interface, an external communication interface with the exterior, and a data storage means with a terminal, and directs to store in said storage means the data received by said external communication interface, without minding a terminal.
[Claim 20] The instruction which directs to output outside the data stored in said storage means in response to the data demand which is the instruction taken out from a terminal to the dual function card which contains a terminal communication interface, an external communication interface with the exterior, and a data storage means with a terminal, and is inputted from said external communication interface, without minding a terminal.
[Claim 21] The instruction which is an instruction taken out from a terminal to the dual function card which contains a terminal communication interface, an external communication interface with the exterior, and a data storage means with a terminal, and is characterized by making two or more actuation perform on a dual function card based on one instruction.
[Claim 22] The data output approach which is an output method of the in-house data of the dual function card which contains a terminal communication interface, an external communication interface with the exterior, and a data storage means with a terminal, and is characterized by outputting outside the data stored in said storage means in response to the data output directions from a terminal, without minding said terminal.
[Claim 23] The data output approach according to claim 22 characterized by performing actuation which reads data from said storage means, and actuation which outputs said data from said external communication interface in response to the instruction which outputs outside the data stored with said storage means from a terminal, without minding a terminal.
[Claim 24] The data-storage approach characterized by to store the data which show a terminal the contents presentation data which are the storing approach of the external data of the dual function card which contains a terminal communication interface, an external communication interface with the exterior, and a data storage means with a terminal, and express the contents of the data inputted from said external communication interface, and store in said storage means in response to the storing directions from a terminal, without minding said terminal.
[Claim 25] It is the written data-storage approach to claim 24 characterized by to perform actuation which stores said data in said storage means in response to the instruction which stores in said storage means the data received by said external communication interface, without minding a terminal from the actuation which creates said contents presentation data and is shown to a terminal when data input from said external communication interface, and a terminal.
[Claim 26] A terminal communication interface with a terminal, and an external communication interface with the exterior, When the data demand of the data which are the output method of the in-house data of the dual function card which contains a data storage means, and were stored in said storage means from said external communication interface is inputted, The data output approach characterized by showing a terminal the contents presentation data showing the contents of the corresponding data, and outputting said data outside in response to the data output directions from a terminal, without minding said terminal.
[Claim 27] The actuation which reads the demanded data from said storage means when a data demand inputs from said external communication interface, From a terminal the data stored in said storage means in response to the external data demand with the actuation which creates said contents presentation data and is shown to a terminal The data output approach according to claim 26 characterized by performing actuation which outputs said data from said external communication interface in response to the instruction outputted outside, without minding a terminal.
[Claim 28] The data output approach according to claim 22 or 26 characterized by enciphering said data and outputting outside.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] Especially this invention relates to the configuration of the dual function card which has an external communication interface in addition to the memory which memorizes data, and a contact with a terminal about a memory card.
[0002]
[Description of the Prior Art] (Conventional technical example 1) An IC card is used for a commuter pass, a telephone card, an ATM card, etc., and both sides -- a memory card is used for PC (personal computer), the storage of a digital camera and a music player, etc. -- are various, and are used in recent years. The memory card is used compensating built-in storage regions, such as a digital camera and a music player, and for the purpose of portability. For example, the image data photoed with the digital camera is memorized to the memory card with which it has equipped, and perusal of said image is attained on PC by equipping PC with this memory card. By PCMCIA specification, it connects with PC and the interface card with external communication interfaces other than a terminal is used as a modem card, a LAN card, etc. Thereby, also in PC which does not contain functions, such as a modem and LAN, data communication with the exterior becomes possible.
[0003] As a hard configuration, the conventional dual function card (henceforth DF card) which contains memory and an external communication interface is equipped with the flash memory 33 which memorizes data, the memory controller 31 which controls read-out/writing of the data of a flash memory 33 according to the directions from a terminal 20, and the IO controller 34 which controls I/O of the data to the exterior according to the directions from a terminal 20, as shown in drawing 14 . As functional block of this DF card 30 is shown in drawing 15 The communication link with a terminal The terminal communication interface Z-15 to perform and the instruction received from the terminal The instruction-execution means Z-11 and data to perform Read-out/writing of the commo data to a storage means Z-13 to hold, a storage control means Z-12 to perform read-out/writing of the data to the storage means Z-13, the external communication interface Z-16 that performs data communication with card external devices other than a terminal, and an external communication interface It consists of external communications control means Z-14 to perform.
[0004] Among these, the instruction-execution means Z-11 and the storage control means Z-12 are functions which the memory controller 31 has, and the storage means Z-13 supports to a flash memory 33, and the external communications control means Z-14 supports the IO controller 34. First, in this DF card, when it is going to output the data held in the storage means Z-13 from the external communication interface Z-16, the sequence shown by drawing 16 (Y-01) - (Y-05) the arrow head is followed.
(Y-01): The instruction issue means Z-21 of a terminal publishes an instruction, and transmits to DF card.
- (Y-03): (Y-02) The instruction-execution means Z-11 which received the instruction from a terminal requires processing of the storage control means Z-12, and takes out data from the storage means Z-13.
(Y-04): The instruction-execution means Z-11 transmits the data taken out from the storage means Z-13 to a terminal as answerback to the instruction from a terminal.
(Y-05): The instruction issue means Z-21 outputs the data received from DF card to the card exterior from the external communications control means Z-14.
Moreover, drawing 17 shows the flow (**-**) of directions to memory, and the data flow (**-**) read from memory on the hard configuration. As mentioned above, the corresponding data must once be taken out from the interior of a card by the terminal to output the data inside DF card to the card exterior.
[0005] (Conventional technical example 2) When it is going to store in the storage means Z-13 the data received from the external communication interface Z-16 in this DF card again, the sequence shown by drawing 18 (X-01) - (X-06) the arrow head is followed.
: (X-01) The external communications control means Z-14 of DF card receives the data from the outside.
: (X-02) The external communications control means Z-14 transmits received data to a terminal.
: (X-03) The terminal which received data from DF card with the instruction issue means Z-21 displays received data to the user of a terminal or DF card, and it goes into the waiting state of actuation (propriety of storing for the storage means Z-13 of received data) of the degree by the user.
: (X-04) The instruction issue means Z-21 publishes an instruction, and transmits the terminal which received the next actuation (storing for the storage means Z-13 of received data is possible) from the user to DF card. In addition, the instruction here contains the received data from DF card inside.
: (X-05) The instruction-execution means Z-11 which received the instruction from a terminal requires processing of the storage control means Z-12, and stores in the storage means Z-13 the received data from DF card outside included inside the instruction.
: (X-06) The instruction-execution means Z-11 transmits the result of data storage processing as answerback to the instruction from a terminal.
In addition, in - (X-03) (X-04), without granting the actuation authority for performing the next actuation to the user of a terminal or DF card, also when automatic performs all, it is possible. Moreover, drawing 19 The directions and data flow (**-**) to memory are shown on the hard configuration. The data flow (**-**) on the hard configuration at this time is shown.
[0006] As mentioned above, the data received from the outside must once go via a terminal to store data in the interior of a card from DF card exterior. Moreover, when it automates altogether as mentioned above in - (X-03) (X-04), the user of a terminal or DF card will be

possible [storing in the interior of a card the data which do not desire storing].
[0007] (Conventional technical example 3) In this DF card, by the demand from the outside which is not a terminal, when it is going to output the data held in the storage means Z-13 from the external communication interface Z-16, the sequence shown by drawing 20 (W-01) - (W-06) the arrow head is followed again.
(W-01): The external communications control means Z-14 receives the notice of a demand from DF card exterior.
(W-02): The external communications control means Z-14 transmits the notice of a demand to a terminal.
(W-03): An instruction issue means Z-21 by which the notice of a demand was received publishes the instruction for outputting applicable data, and transmits it to DF card.
: (W-04-W-05) The instruction-execution means Z-11 which received the instruction from a terminal requires processing of the storage control means Z-12, and takes out data from the storage means Z-13.
(W-06): The instruction-execution means Z-11 transmits the data taken out from the storage means Z-13 to a terminal as answerback to the instruction from a terminal.
(W-07): The instruction issue means Z-21 outputs the data received from DF card to the card exterior from the external communications control means Z-14.
[0008] In addition, in (W-03), to the user of a terminal or DF card, also when urging the actuation to the following activation of operation, it is possible. Moreover, drawing 21 shows the flow (**-**) of directions to memory, and the data flow (**-**) read from memory on the hard configuration. As mentioned above, applicable data must once go via a terminal to output the data inside a card by the demand from DF card outside. Furthermore, it will also become possible to output the data which the user of a terminal or DF card does not desire to the card exterior.
[0009] (Conventional technical example 4) Next, in the conventional IC card (a contact interface and a non-contact interface is not asked here), the case where the data inside a card are taken out to a terminal is explained. As shown in drawing 22 , an IC card consists of the terminal communication interface V-14 which performs the communication link with a terminal, an instruction-execution means V-11 to execute the instruction received from the terminal, a storage means V-13 to hold data, and a storage control means V-12 to perform read-out/writing of the data to the storage means Z-13. In this IC card, when a terminal tends to read the data held in the storage means V-13, the sequence shown by drawing 22 (V-01) - (V-04) the arrow head is followed.
: (V-01) The instruction issue means V-21 of a terminal publishes an instruction, and transmits to an IC card.
- (V-03): (V-02) The instruction-execution means V-11 which received the instruction from a terminal requires processing of the storage control means V-12, and takes out data from the storage means V-13.
: (V-04) The instruction-execution means V-11 transmits the data taken out from the storage means V-13 to a terminal as answerback to the instruction from a terminal.
As mentioned above, when taking out the data inside an IC card to a terminal, once an instruction is published with a terminal, processing termination cannot perform decision of grasp of the contents of the data to take out by the card user, interruption of actuation (read-out of data), etc.
[0010]
[Problem(s) to be Solved by the Invention] Since in the case of DF card in (the conventional technical example 1) it cannot output outside unless it is after once passing the data in storage means Z-13 to a terminal, when treating important data (for example, a credit card number, cybermoney, etc.), it must be guaranteed that a terminal does not carry out unjust actuation. With unjust actuation of a terminal here, unjust alteration, are recording, deletion, etc. of data are mentioned.
[0011] Moreover, since in DF card in (the conventional technical example 2) it cannot output outside unless it comes out, once it passes the received data from the card outside to a terminal, the same technical problem as the thing in (the conventional technical example 1) is mentioned. Furthermore, there is risk of the data which the user of a terminal or DF card does not desire being stored inside a card.
[0012] Similarly, in order once to have to pass the both sides of the data in the demand from the card outside, and storage means Z-13 to a terminal also in DF card in (the conventional technical example 3), the same technical problem as the thing in (the conventional technical example 1) is mentioned. Furthermore, there is risk of outputting the data which the user of a terminal or DF card does not desire to the card exterior. Moreover, since a card user does not know till processing termination which data are taken out with the instruction which the terminal published in the case of the IC card in (the conventional technical example 4), it must be guaranteed that a terminal does not carry out unjust actuation.
[0013] This invention aims at solving such a technical problem, and eliminating room for the unjust actuation by the terminal intervening, and preventing the unjust writing and unjust read-out of data from the outside, and offering DF card which can hold the secrecy nature and the integrity of are recording data, and offering the data output approach of this DF card, and the data storage approach.
[0014]
[Means for Solving the Problem] So, in this invention, it sets on DF card which contains a terminal communication interface, an external communication interface with the exterior, and a data storage means with a terminal. An instruction-execution means to execute the instruction received from the terminal communication interface or the external communication interface, A storage control means to control writing and read-out of data for a storage means in response to the instruction of an instruction-execution means, and an external communications control means to control I/O of the commo data from an external communication interface in response to the instruction of an instruction-execution means are established.
[0015] Moreover, he is trying to output outside the data stored in the storage means in response to the data output directions from a terminal in the data output approach of this DF card, without minding a terminal. Moreover, he shows a terminal the contents presentation data showing the contents of the data inputted from an external communication interface, and is trying to store the data stored in a storage means in response to the storing directions from a terminal in the data storage approach of this DF card, without minding a terminal. Moreover, when the data demand of the data stored in the storage means from the external communication interface is inputted, he shows a terminal the contents presentation data showing the contents of the corresponding data, and is trying to output this data outside in response to the data output directions from a terminal in the data output approach of this DF card, without minding a terminal.
[0016] DF card which prevented the unjust actuation by the terminal can be constituted by this, and the secrecy nature and the integrity of a card in-house data can be held. Moreover, the secrecy nature and the integrity of output data are held by outputting outside the data saved in the interior of DF card, without minding a terminal. Moreover, the secrecy nature and the integrity of input data are held by saving input data in the interior of DF card, without minding a terminal. Moreover, the secrecy nature and the integrity of output data are held by

outputting outside the data saved in the interior of DF card by making the input from the outside DF card and other than a terminal into a trigger, without minding a terminal.

[0017]

[Embodiment of the Invention] (1st operation gestalt) The 1st operation gestalt explains the whole secure DF card configuration and actuation in this invention. As a hard configuration, the secure DF card in the operation gestalt of this invention is equipped with read-out / DF controller 11 which writes in and controls the data input/output operation of the DFIO controller 14 of the data of a flash memory 13 in response to the flash memory 13 which memorizes data, the DFIO controller 14 which controls I/O of data with the exterior, and the directions from a terminal 20, as shown in drawing 1 .

[0018] Functionally, as shown in drawing 2 , this DF card Data communication with a terminal A-20 The terminal communication interface A-15 to perform, an instruction-execution means A-11 to execute the instruction received from the terminal A-20, a storage means A-13 to hold data, a storage control means A-12 to perform read-out/writing of the data to the storage means A-13, It consists of external communications control means A-14 to perform read-out/writing of the commo data to the external communication interface A-16 and the external communication interface A-16 which perform data communication with card external devices other than terminal A-20. Among these, the instruction-execution means A-11 and the storage control means A-12 are functions which the DF controller 11 has, and the storage means A-13 supports to a flash memory 13, and the external communications control means A-14 supports the DFIO controller 14.

[0019] This instruction-execution means A-11 and the storage control means A-12 constitute each inside one IC chip as a software module, and give tamper-proof nature in hardware. Even if the storage means A-13 is a flash memory without tamper-proof nature by carrying out like this, the secrecy nature of the data written in the storage means A-13 can be held by enciphering the data written in the storage means A-13 with the instruction-execution means A-11.

[0020] Moreover, when IC-izing the instruction-execution means A-11 and the storage control means A-12, the external communications control means A-14 may also be constituted inside the IC chip same as a software module. In this case, the instruction-execution means A-11, the storage control means A-12, and the external communications control means A-14 can be constituted as one IC chip which has tamper-proof nature in hardware. Moreover, you may constitute inside one chip with tamper-proof nature by making each of the instruction-execution means A-11, the storage control means A-12, and the external communications control means A-14 into hardware. Moreover, the instruction-execution means A-11 is constituted as software on a tamper-proof nature IC chip, and the storage control means A-12 and the external communications control means A-14 are mounted as hardware, and you may make it give tamper-proof nature. By taking this configuration, the hardware which constitutes the storage control means and external communications control means which were used with the conventional card can be diverted to the secure DF card of this invention.

[0021] In this secure DF card, the instruction-execution means A-11 interprets the card control instruction which the instruction issue means A-21 published, and requires processing from the storage control means A-12 or the external communications control means A-14 according to those contents. Moreover, the card control response to card control instruction is returned to a terminal A-20. The storage control means A-12 performs read-out/writing of data to the field where the A-storage means 13 interior was specified based on the processing demand from the instruction-execution means A-11.

[0022] The external communications control means A-14 inputs the data which received the specified data to the external communication interface A-16 at the output or the external communication interface A-16 into the instruction-execution means A-11 based on the processing demand from the instruction-execution means A-11. The terminal communication interface A-15 has a contact with the card communication interface A-22 of a terminal A-20, and performs serial communication between a terminal A-20 and the secure DF card A-10. The external communication interface A-16 performs data communication with external devices other than terminal A-20 according to control of the external communications control means A-14. This interface corresponds to radio specification, such as infrared radiation and Bluetooth-ISO14443, and wire communication specification, such as IEEE1394 and USB, and the external communications control means A-14 serves as a module for controlling based on the telecommunications standard to which the external communication interface A-16 corresponds.

[0023] Moreover, the terminal A-20 in the operation gestalt of this invention consists of a card communication interface A-22 which performs data communication with the secure DF card A-10, and an instruction issue means A-21 to publish card control instruction to the secure DF card A-10, as shown in drawing 2 . This terminal A-20 is a personal computer, remote control of a cellular phone and television, etc. The secure DF card A-10 operates, when the card control instruction which the instruction issue means A-21 of a terminal A-20 published is received through the card communication interface A-22 and the terminal communication interface A-15 and the instruction-execution means A-11 executes the instruction.

[0024] Here the card control instruction which the instruction issue means A-21 publishes The data received from the outside by the <card control instruction 2> external communication interface A-16 which outputs to the exterior the data which the <card control instruction 1> storage means A-13 holds from the external communication interface A-16, without minding a terminal A-20 By the demand from the A-secure DF card 10 outside other than <card control instruction 3> terminal A-20 inputted into the storage means A-13, without minding a terminal A-20 Suppose that they are three kinds of outputting the data which the storage means' A-'s13 holds to the exterior from the external communication interface A-16, without minding a terminal A-20.

[0025] Below, a detail is explained about actuation when the secure DF card A-10 receives <the card control instruction 1>. In drawing 3 , the basic format of the response to which instruction-execution means A-11, storage control means A-12, and the external communications control means A-14 publish to (A) a basic format of the instruction which instruction issue means A-21 and the instruction-execution means A-11 publish is shown in (B). In drawing 3 (A), the instruction identifier C-01 expresses the identifier showing the instruction ending the class of instruction, data [need / the data length of an instruction and the contents C-03 of an instruction / for activation of the instruction / an instruction length C-02], and the instruction termination identifier C-04, respectively. Moreover, in drawing 3 (B), the identifier to which the response identifier C-11 means that the response ends the class of response, the data showing an activation result [as opposed to / length / C-12 / response / an instruction in the data length of a response and the contents C-13 of a response], and the response termination identifier C-14 is expressed, respectively.

[0026] Next, the structure of <response 1> over <instruction 1> and it in this operation gestalt is shown in drawing 4 at (A) - (F), respectively. Drawing 4 (A) expresses the <card control instruction 1> which the instruction issue means A-21 publishes. D-01 corresponds to the instruction identifier C-01, and turns into "00001001" in <the card control instruction 1>. D-02 corresponds to an instruction length C-02, and shows the die length of <the card control instruction 1>. Start-address D-03 and a data length D-04 support the contents C-03 of an instruction. A start address D-03 shows the start address (logical address) of the data outputted from the external communication

interface A-16 currently held to the A-storage means 13 interior by <the card control instruction 1>. A data length D-04 shows the die length of the data outputted from the external communication interface A-16 currently held to the A-storage means 13 interior. D-05 corresponds to the instruction termination identifier C-04, and is set to "10001001" by <the card control instruction 1>.
[0027] Drawing 4 (B) expresses the <card control response 1> which the instruction-execution means A-11 publishes. D-11 corresponds to the response identifier C-11, and is set to "00001010" by <the card control response 1>. D-12 corresponds to the response length C-12, and shows the die length of <the card control response 1>. The processing result D-13 corresponds to the contents C-13 of a response, and the sequence of numbers which shows a success ("00000000") or failure ("11111111") of an activation result in <the card control instruction 1> enters. D-14 corresponds to the response termination identifier C-14, and is set to "10001010" by <the card control response 1>.
[0028] Drawing 4 (C) expresses the <storage control instruction 1> which the instruction-execution means A-11 publishes. D-21 corresponds to the instruction identifier C-01, and is set to "00001011" by <the storage control instruction 1>. D-22 corresponds to an instruction length C-02, and shows the die length of <the storage control instruction 1>. Start-address D-23 and a data length D-24 support the contents C-03 of an instruction. The semantics which start-address D-23 and a data length D-24 have is the same as that of start-address D-03 and the data length D-04 in <the card control instruction 1>. D-25 corresponds to the instruction termination identifier C-04, and is set to "10001011" by <the storage control instruction 1>.
[0029] Drawing 4 (D) expresses the <storage control response 1> which the storage control means A-12 publishes. D-31 corresponds to the response identifier C-11, and is set to "00001100" by <the storage control response 1>. D-32 corresponds to the response length C-12, and shows the die length of <the storage control response 1>. Data length D-33 and the body D-34 of data support the contents C-13 of a response. A data length D-33 shows the die length of the following body D-34 of data. The body D-34 of data is specified with <the storage control instruction 1>, and the body of the data taken out from the storage means A-13 enters. D-35 corresponds to the response termination identifier C-14, and is set to "10001100" by <the storage control response 1>.
[0030] Drawing 4 (E) expresses the <communications control instruction 1> which the instruction-execution means A-11 publishes. D-41 corresponds to the instruction identifier C-01, and is set to "00001101" by <the communications control instruction 1>. D-42 corresponds to an instruction length C-02, and shows the die length of <the communications control instruction 1>. Data length D-43 and the body D-44 of data support the contents C-03 of an instruction. The semantics which data length D-43 and the body D-44 of data have is the same as that of data length D-33 and the body D-34 of data in <the storage control response 1>. D-45 corresponds to the instruction termination identifier C-04, and is set to "10001101" by <the communications control instruction 1>.
[0031] Drawing 4 (F) expresses the <communications control response 1> which the external communications control means A-14 publishes. D-51 corresponds to the response identifier C-11, and is set to "00001110" by <the communications control response 1>. D-52 corresponds to the response length C-12, and shows the die length of <the communications control response 1>. The processing result D-53 corresponds to the contents C-13 of a response, and the sequence of numbers which shows a success ("00000000") or failure ("11111111") of an activation result in <the communications control instruction 1> enters. D-54 corresponds to the response termination identifier C-14, and is set to "10001110" by <the communications control response 1>.
[0032] Next, actuation in the A-secure DF card 10 interior is explained. Drawing 5 simplifies and shows the data flow (**-**) read from the flow (**-**) of directions and memory 13 to the memory 13 in the case of outputting outside the data held by the memory 13 of the secure DF card 10 based on the directions from a terminal 20 on the hard configuration of a secure DF card.
[0033] Drawing 6 shows this detail. In drawing 6 , the figure enclosed with an arrow head and a parenthesis shows typically procedure when the secure DF card A-10 receives <the card control instruction 1> from a terminal A-20. (B-01): The instruction issue means A-21 of a terminal A-20 publishes <card control instruction 1>, and transmits to the secure DF card A-10.
[0034] (B-02): An instruction-execution means A-11 of the secure DF card A-10 by which <the card control instruction 1> was received <Card control instruction 1> is interpreted (here). It checks that the check of the die length of <the card control instruction 1>, reading of start-address D-03 and a data length D-04, and the part of D-05 are "10001001" from the check of the part of D-01 being "00001001", and the part of D-02. Next, the instruction-execution means A-11 generates <the storage control instruction 1>, and transmits it to the storage control means A-12.
[0035] (B-03-B-04) The storage control means A-12 which received : <the storage control instruction 1> <The storage control instruction 1> is interpreted (here). It checks that the check of the part of D-21 being "00001011", the check of the die length of the part of D-22 to the <storage control instruction 1>, reading of start-address D-23 and a data length D-24, and the part of D-25 are "10001011." Next, the storage control means A-12 takes out the data specified from the start address D-23 described at <the storage control instruction 1>, and the data length D-24 from the storage means A-13.
[0036] (B-05): The storage control means A-12 generates <the storage control response 1> from the data taken out from the storage means A-13, and transmits it to the instruction-execution means A-11.
(B-06): The instruction-execution means A-11 which received <the storage control response 1> interprets <the storage control response 1> (here, it checks that the check of the part of D-31 being "00001100", the check of the die length of the part of D-32 to the <storage control response 1>, reading of data length D-33 and the body D-34 of data, and the part of D-35 are "10001100"). Next, the instruction-execution means A-11 generates <the communications control instruction 1> from data length D-33 and the body D-34 of data, and transmits it to the external communications control means A-14. In addition, the instruction-execution means A-11 enciphers the body D-44 of data, and you may make it include it into <the communications control instruction 1> at this time.
[0037] (B-07): An external communications control means A-14 by which <the communications control instruction 1> was received interprets <the communications control instruction 1> (here, it checks that the check of the part of D-41 being "00001101", the check of the die length of the part of D-42 to the <communications control instruction 1>, reading of data length D-43 and the body D-44 of data, and the part of D-45 are "10001101"). Next, the external communications control means A-14 outputs the body D-44 of data included in <the communications control instruction 1> from the external communication interface A-16 to the exterior of the secure DF card A-10. In addition, when the body D-44 of data is enciphered by the instruction-execution means A-11, that decryption is performed at the point which received this body D-44 of data.
[0038] (B-08): After the output to the exterior of the target data is completed, the external communications control means A-14 generates <the communications control response 1>, and transmits it to the instruction-execution means A-11.
(B-09): The instruction-execution means A-11 which received <the communications control response 1> interprets <the communications control response 1> (here, it checks that the check of the part of D-51 being "00001110", the check of the die length of the part of D-52 to the <communications control response 1>, reading of the processing result D-53, and the part of D-54 are "10001110"). Next, based on the

processing result D-53 included in <the communications control response 1>, the instruction-execution means A-11 generates <the card control response 1>, is transmitting to a terminal A-20, and notifies the processing result of <the card control instruction 1> to a terminal A-20.

[0039] (B-10): An instruction issue means A-21 by which <the card control response 1> was received interprets <the card control response 1> (here, it checks that the check of the part of D-11 being "00001010", the check of the die length of the part of D-12 to the <card control response 1>, reading of the processing result D-13, and the part of D-14 are "10001010"). When the instruction issue means A-21 verifies the contents of this processing result D-13, a terminal A-20 checks the activation result of <the card control instruction 1>.

[0040] The point which should be noted here is that the instruction-execution means A-11 of this secure DF card A-10 performs two or more actuation in response to one instruction from the instruction issue means A-21 of a terminal A-20. That is, if <the card control instruction 1> is received from the instruction issue means A-21 of a terminal A-20, <the storage control instruction 1> will be generated, and data will be read from the storage means A-13, and <the communications control instruction 1> will be generated, and data will be outputted outside from the external communication interface A-16.

[0041] Although only one actuation will usually be performed with the conventional card which operates passively if one instruction is received The instruction-execution means A-11 of this secure DF card A-10 is performing two or more actuation to one instruction, and it enables this to output the data which it has in the A-storage means 13 interior to the A-secure DF card 10 exterior, without mediating a terminal A-20. In addition, a format of the above-mentioned instruction is one example, and may use other formats.

[0042] In case a terminal A-20 outputs outside the data recorded on the memory of a secure DF card by making the above processings perform in the A-secure DF card 10 interior, the concern by which data are unjustly operated with a terminal is wiped away. Therefore, it becomes possible to perform electronic commerce by the Internet etc., equipping a cellular phone, remote control of a digital television, etc. with this secure DF card, storing the data which require secrecy, such as cybermoney, a credit card number, and individual humanity news, at the memory of a secure DF card, and looking at the screen of a cellular phone or television.

[0043] The card itself does not perform such processing, but when possibility of carrying out unjust actuation of the data at a terminal is left behind, a guarantee to which such injustice is not carried out will be called for from a terminal. This complicates the function of a terminal and makes the rise of cost unavoidable. However, a terminal can escape such duty by using this secure DF card.

[0044] Drawing 7 shows the procedure in the case of settling purchase goods as such an example using the credit card information in the secure DF card A-10 with which the personal digital assistant A-20 was equipped. First, the user who purchased goods at the store receives a settlement-of-accounts demand from a store (1). A user operates a possession card check from a personal digital assistant A-20 (2). In response, a possession card information confirmatory order is taken out from the instruction issue means A-21 of a terminal to the instruction-execution means A-11 of the secure DF card A-10 (3). All the possession card information that issued the instruction and was read from (4) and the storage means A-13 so that all possession card information might be read to the storage control means A-12 is sent to the instruction issue means A-21 of a terminal through the instruction-execution means A-11, and the instruction-execution means A-11 is displayed on the screen of (5) and a terminal A-20 (6).

[0045] The user who looked at the screen determines a use card out of a possession card, and performs (7) use card assignment actuation (8). In response, the instruction issue means A-21 of a terminal gives the output instruction of an operating card number to the instruction-execution means A-11 of the secure DF card A-10 (9). The instruction-execution means A-11 is ordered to read the specified operating card number to the storage control means A-12, and if the operating card number read from the storage means A-13 is acquired, (10) and the external communications control means A-14 will be ordered to output the operating card number (11). The external communications control means A-14 transmits an operating card number to a store from the external communication interface A-16 according to the instruction (12). At a store, the effectiveness of the card is checked, (13) and settlement of accounts are performed, and the notice of settlement-of-accounts termination is published (14).

[0046] Thus, this secure DF card A-10 can perform it, without mediating a terminal A-20, when outputting outside the data which it has in the A-storage means 13 interior through the external communication interface A-16.

[0047] In addition, although this operation gestalt shows the case where instruction issue of a terminal and a card interior action are performed seamlessly, it is good also as placing and realizing instruction issue and a card interior action for time difference. The processing which this says a cybermoney output instruction is published from a contact interface with a cellular phone, and it removes and walks around with the IC card, and performs settlement-of-accounts processing to a payment machine with a non-contact interface in an IC card with both interface contact/non-contact one is attained. [for example,] Furthermore, this IC card can also hang the limit which is the instruction received beforehand and which is said that it pays and only processing is made to be not possible to a payment machine.

[0048] (2nd operation gestalt) The 2nd operation gestalt explains a detail about the actuation at the time of receiving until the secure DF card A-10 receives <the card control instruction 2> from a terminal A-20. The structure of other transmitted and received datas is shown in the <instruction 2> in this operation gestalt and <response 2>, and a pan as (A) - (G) at drawing 10 , respectively.

[0049] Drawing 10 (A) expresses the <received data 1> which the external communication interface A-16 receives from the secure DF card A-10 exterior. G-01 differs for every received data in a header each time. The received-data length G-02 shows the die length of <received data 1>. The body G-03 of data shows the body of data to store in the storage means A-13. The termination identifier G-04 is an identifier which shows that <received data 1> are completed.

[0050] Drawing 10 (B) expresses the <data receipt 1> which the external communications control means A-14 publishes. G-11 corresponds to the instruction identifier C-01, and turns into "00100111" in <the data receipt 1>. Message length G-12 corresponds to an instruction length C-02, and shows the die length of <the data receipt 1>. Data G-13 correspond to the contents C-03 of an instruction, and serve as the body G-03 of data in <received data 1>. G-14 corresponds to the instruction termination identifier C-04, and is set to "10100111" by <the data receipt 1>.

[0051] Drawing 10 (C) expresses the <data receipt 2> which the instruction-execution means A-11 publishes. G-21 corresponds to the instruction identifier C-01, and is set to "00101000" by <the data receipt 2>. Message length G-22 corresponds to an instruction length C-02, and shows the die length of <the data receipt 2>. Index G-23 and the body length G-24 of data support the contents C-03 of an instruction. An index G-23 is index data generated from the body G-03 of data in <received data 1>. The body length G-24 of data shows the die length of the body G-03 of data in <received data 1>. G-25 corresponds to the instruction termination identifier C-04, and is set to "10101000" by <the data receipt 2>.

[0052] Drawing 10 (D) expresses the <card control instruction 2> which the instruction issue means A-21 publishes. G-31 corresponds to the instruction identifier C-01, and is set to "00100001" by <the card control instruction 2>. G-32 corresponds to an instruction length C-

02, and shows the die length of <the card control instruction 2>. Start-address G-33 and a data length G-34 support the contents C-03 of an instruction. A start address G-33 shows the start address (logical address) of the storing location of the body G-04 of data saved in the A-storage means 13 interior by <the card control instruction 2>. Since the body G-04 of data is stored, a data length G-34 shows the area size secured in the storage means A-13. G-35 corresponds to the instruction termination identifier C-04, and is set to "10100001" by <the card control instruction 2>.

[0053] Drawing 10 (E) expresses the <card control response 2> which the instruction-execution means A-11 publishes. G-41 corresponds to the response identifier C-11, and is set to "00100010" by <the card control response 2>. G-42 corresponds to the response length C-12, and shows the die length of <the card control response 2>. The processing result G-43 corresponds to the contents C-13 of a response, and the sequence of numbers which shows a success ("00000000") or failure ("11111111") of an activation result in <the card control instruction 2> enters. G-44 corresponds to the response termination identifier C-14, and is set to "10100010" by <the card control response 2>.

[0054] Drawing 10 (F) expresses the <storage control instruction 2> which the instruction-execution means A-11 publishes. G-51 corresponds to the instruction identifier C-01, and is set to "00100011" by <the storage control instruction 2>. G-52 corresponds to an instruction length C-02, and shows the die length of <the storage control instruction 2>. Start-address G-53 and a data length G-54 support the contents C-03 of an instruction. A start address G-53 shows the start address (logical address) of the storing location of the body G-04 of data saved in the A-storage means 13 interior with <the storage control instruction 2>. Since the body G-04 of data is stored, a data length G-54 shows the area size secured in the storage means A-13. G-55 corresponds to the instruction termination identifier C-04, and is set to "10100011" by <the storage control instruction 2>.

[0055] Drawing 10 (G) expresses the <storage control response 2> which the storage control means A-12 publishes. G-61 corresponds to the response identifier C-11, and is set to "00100100" by <the storage control response 2>. G-62 corresponds to the response length C-12, and shows the die length of <the storage control response 2>. The processing result G-63 corresponds to the contents C-13 of a response, and the sequence of numbers which shows a success ("00000000") or failure ("11111111") of an activation result in <the storage control instruction 2> enters. G-64 corresponds to the response termination identifier C-14, and is set to "10100100" by <the storage control response 2>.

[0056] Next, actuation in the A-secure DF card 10 interior is explained. Drawing 8 simplifies and shows the data flow in the case of storing in the memory 13 of the secure DF card 10 the data inputted from the outside (**, **, **), and the flow (**, **) which waits for directions of a user through a terminal 20 on the hard configuration of a secure DF card.

[0057] Drawing 9 shows this procedure to the detail, and in drawing 9 R> 9, the figure enclosed with an arrow head and a parenthesis shows the procedure after reception typically until the secure DF card A-10 receives <the card control instruction 2> from a terminal A-20.

(E-01): The external communications control means A-14 receives <received data 1> from the A-secure DF card 10 exterior.

(E-02): An external communications control means A-14 by which <received data 1> were received interprets <received data 1> (here, the check of the die length of <received data 1>, reading of the body G-03 of data, and the check of the termination identifier G-04 are performed from the check of a header G-01, and the part of G-02). Next, the external communications control means A-14 generates <the data receipt 1>, and transmits it to the instruction-execution means A-11.

[0058] (E-03): The instruction-execution means A-11 which received <the data receipt 1> interprets <the data receipt 1> (here, it checks that the check of the die length of <the data receipt 1>, reading of data G-13, and the part of G-14 are "10100111" from the check of the part of G-11 being "00100111", and the part of G-12). Next, from the body G-03 of data, the instruction-execution means A-11 generates an index G-23 as contents presentation data showing the contents of data, generates <the data receipt 2> based on it, and transmits it to a terminal A-20. In addition, generation of an index G-23 is performed by extracting some bodies G-03 of data.

[0059] (E-04): An instruction issue means A-21 by which <the data receipt 2> was received interprets <the data receipt 2> (here, it checks that the check of the die length of <the data receipt 2>, reading of index G-23 and the body length G-24 of data, and the part of G-25 are "10101000" from the check of the part of G-21 being "00101000", and the part of G-22). Next, a terminal A-20 displays an index G-23 to the user of a terminal A-20 or the secure DF card A-10, and goes into the waiting state of actuation (propriety of storing for the storage means A-13 of received data) of the degree by the user.

[0060] (E-05): At the terminal A-20 which received the next actuation (storing for the storage means A-13 of received data is possible) from the user, the instruction issue means A-21 publishes <card control instruction 2>, and transmits to the secure DF card A-10.

(E-06): The instruction-execution means A-11 which received <the card control instruction 2> interprets <card control instruction 2> (here, it checks that the check of the die length of <the card control instruction 2>, reading of start-address G-33 and a data length G-34, and the part of G-35 are "10100001" from the check of the part of G-31 being "00100001", and the part of G-32). Next, the instruction-execution means A-11 generates <the storage control instruction 2> from the body G-03 of data received from the external communications control means A-14, and transmits it to the storage control means A-12. At this time, the instruction-execution means A-11 may encipher the body G-03 of data.

[0061] (E-07): The storage control means A-12 which received <the storage control instruction 2> <The storage control instruction 2> is interpreted (here). It checks that reading of start-address G-53, data length G-54, and the body G-55 of data and the part of G-56 are "10100011." Next, in the storage means A-13, the storage control means A-12 secures the field of the die length of a data length G-54 from a start address G-53, and stores the body G-55 of data.

[0062] (E-08): The storage control means A-12 generates <the storage control response 2>, and transmits it to the instruction-execution means A-11.

(E-09): The instruction-execution means A-11 which received <the storage control response 2> interprets <the storage control response 2> (here, it checks that the check of the part of G-61 being "00100100", the check of the die length of the part of G-62 to the <storage control response 2>, reading of the processing result G-63, and the part of G-64 are "10100100"). Next, based on the processing result G-63 included in <the storage control response 2>, the instruction-execution means A-11 generates <the card control response 2>, is transmitting to a terminal A-20, and notifies the processing result of <the card control instruction 2> to a terminal A-20.

[0063] (E-10): An instruction issue means A-21 by which <the card control response 2> was received interprets <the card control response 2> (here, it checks that the check of the part of G-41 being "00100010", the check of the die length of the part of G-42 to the <card control response 2>, reading of the processing result G-43, and the part of G-44 are "10100010").

[0064] In this case, the instruction-execution means A-11 performs two, the actuation which generates an index G-23 from the body G-03 of data, generates <the data receipt 2> as actuation corresponding to the one <card control instruction 2> which a terminal outputs, and is

shown to a terminal A-20, and the actuation which generates <the storage control instruction 2> and stores data in a storage means. In addition, a format of the above-mentioned instruction is one example, and may use other formats.
[0065] Data are stored in the A-storage means 13 interior, after telling only the index to the terminal A-20 and checking a user's volition, when data are received from the external communication interface A-16 by making the above processings perform in the A-secure DF card 10 interior. Therefore, it becomes possible to store in the A-storage means 13 interior the data received from the external communication interface A-16, without mediating a terminal A-20.
[0066] For example, if the receipt data of electronic commerce are sent from an online shop through the external communication interface A-16, the instruction-execution means A-11 will extract "Ox store receipt January 1, 2002" which is data to the 2nd line of the data, and will send it to a terminal. If the user who checked this on the screen of a terminal directs preservation of a receipt, the instruction-execution means A-11 stores in the storage means A-13 the receipt data sent from the outside. Moreover, when a user makes preservation of a receipt unnecessary, he discards receipt data. In this case, to a terminal, since the receipt data itself are not sent, it can prevent beforehand the injustice referred to as that a user altered and holds a receipt.
[0067] In addition, in this operation gestalt, although [instruction issue of a terminal and a card interior action] carried out seamlessly, they are good also as placing and realizing instruction issue and a card interior action for time difference. Thereby, in an IC card with the interface of for example, contact / non-contact both sides, a cybermoney restoration instruction is published from a contact interface with a cellular phone, it removes and walks around with the IC card, and processing of a cybermoney restoration machine with a non-contact interface performing restoration processing is attained. Furthermore, it also becomes possible to apply the limit referred to as, as for this IC card, to be able to be made not to perform only restoration processing which is the instruction received beforehand to a restoration machine.

[0068] Moreover, in this operation gestalt, although only the case where the input data from the outside is stored in a storage means is described, an instruction-execution means takes collating with input data and another data of a storage means, and the gestalt which presupposes that only that result is transmitted to a terminal also has it. It becomes possible to have said that an instruction-execution means collated with the image data of the normal currently held at the storage means, and displayed only the judgment result on a cellular phone from a contact interface by this about the image data inputted from the CCD camera interface in a memory card with both a contact interface with a cellular phone, and the interface to a CCD camera.
[0069] (3rd operation gestalt) The 3rd operation gestalt explains a detail about the actuation at the time of receiving until the secure DF card A-10 receives <the card control instruction 3> from a terminal A-20.
[0070] The structure of other transmitted and received datas is shown in the <instruction 3> in this operation gestalt and <response 3>, and a pan as (A) - (I) at drawing 13 , respectively. Drawing 13 (A) expresses the <received data 2> which the external communication interface A-16 receives from the secure DF card A-10 exterior. J-01 differs for every received data in a header each time. The received-data length J-02 shows the die length of <received data 2>. The output request J-03 shows which data of the data which the secure DF card A-10 has he wants to output. The termination identifier J-04 is an identifier which shows that <received data 2> are completed.
[0071] Drawing 13 (B) expresses the <data receipt 3> which the external communications control means A-14 publishes. J-11 corresponds to the instruction identifier C-01, and turns into "01000111" in <the data receipt 3>. Message length J-12 corresponds to an instruction length C-02, and shows the die length of <the data receipt 3>. Data J-13 correspond to the contents C-03 of an instruction, and are the same as that of the output request J-03 in <received data 2>. J-14 corresponds to the instruction termination identifier C-04, and is set to "11000111" by <the data receipt 3>.
[0072] Drawing 13 (C) expresses the <data receipt 4> which the instruction-execution means A-11 publishes. J-21 corresponds to the instruction identifier C-01, and is set to "01001000" by <the data receipt 4>. Message length J-22 corresponds to an instruction length C-02, and shows the die length of <the data receipt 4>. Index J-23 and a data length J-24 support the contents C-03 of an instruction. An index J-23 is index data which the instruction-execution means A-11 generated based on the output request J-03 about the data taken out from the storage means A-13 with <the storage control instruction 3 <the storage control response 3>>. A data length J-24 shows the die length of data taken out from the storage means A-13 with <the storage control instruction 3 <the storage control response 3>>. J-25 corresponds to the instruction termination identifier C-04, and is set to "11001000" by <the data receipt 4>.
[0073] Drawing 13 (D) expresses the <card control instruction 3> which the instruction issue means A-21 publishes. J-31 corresponds to the instruction identifier C-01, and is set to "01000001" by <the card control instruction 3>. J-32 corresponds to an instruction length C-02, and shows the die length of <the card control instruction 3>. A data length J-33 corresponds to the contents C-03 of an instruction, and shows the die length of the data outputted outside from the storage means A-13. J-34 corresponds to the instruction termination identifier C-04, and is set to "11000001" by <the card control instruction 3>.
[0074] Drawing 13 (E) expresses the <card control response 3> which the instruction-execution means A-11 publishes. J-41 corresponds to the response identifier C-11, and is set to "01000010" by <the card control response 3>. J-42 corresponds to the response length C-12, and shows the die length of <the card control response 3>. The processing result J-43 corresponds to the contents C-13 of a response, and the sequence of numbers which shows a success ("00000000") or failure ("11111111") of an activation result in <the card control instruction 3> enters. J-44 corresponds to the response termination identifier C-14, and is set to "11000010" by <the card control response 3>.
[0075] Drawing 13 (F) expresses the <storage control instruction 2> which the instruction-execution means A-11 publishes. G-51 corresponds to the instruction identifier C-01, and is set to "01000011" by <the storage control instruction 3>. J-52 corresponds to an instruction length C-02, and shows the die length of <the storage control instruction 3>. Start-address J-53 and a data length J-54 support the contents C-03 of an instruction. A start address J-53 shows the start address (logical address) of the data specified by the output request J-03 currently held to the A-storage means 13 interior. A data length J-54 shows the die length of the data specified by the output request J-03 currently held to the A-storage means 13 interior. J-55 corresponds to the instruction termination identifier C-04, and is set to "11000011" by <the storage control instruction 3>.
[0076] Drawing 13 (G) expresses the <storage control response 3> which the storage control means A-12 publishes. J-61 corresponds to the response identifier C-11, and is set to "01000100" by <the storage control response 3>. J-62 corresponds to the response length C-12, and shows the die length of <the storage control response 3>. Data length J-63 and the body J-64 of data support the contents C-13 of a response. A data length J-63 shows the die length of the following body J-64 of data. The body J-64 of data is specified with <the storage control instruction 3>, and the body of the data taken out from the storage means A-13 enters. J-64 corresponds to the response termination identifier C-14, and is set to "11000100" by <the storage control response 3>.
[0077] Drawing 13 (H) expresses the <communications control instruction 3> which the instruction-execution means A-11 publishes. J-71

corresponds to the instruction identifier C-01, and is set to "01000101" by <the communications control instruction 3>. J-72 corresponds to an instruction length C-02, and shows the die length of <the communications control instruction 3>. Data length J-73 and the body J-74 of data support the contents C-03 of an instruction. The semantics which data length J-73 and the body J-74 of data have is the same as that of data length J-63 and the body J-64 of data in <the storage control response 3>. J-75 corresponds to the instruction termination identifier C-04, and is set to "11000101" by <the communications control instruction 3>.

[0078] Drawing 13 (I) expresses the <communications control response 3> which the external communications control means A-14 publishes. J-81 corresponds to the response identifier C-11, and is set to "01000110" by <the communications control response 3>. J-82 corresponds to the response length C-12, and shows the die length of <the communications control response 3>. The processing result J-83 corresponds to the contents C-13 of a response, and the sequence of numbers which shows a success ("00000000") or failure ("11111111") of an activation result in <the communications control instruction 3> enters. J-84 corresponds to the response termination identifier C-14, and is set to "11000110" by <the communications control response 3>.

[0079] Next, actuation in the A-secure DF card 10 interior is explained. The flow of the directions to the memory 13 in the case of outputting outside the data held by the memory 13 of the secure DF card 10, after drawing 11's receiving the demand from the outside and checking a user's volition (**-**), The flow (**-**) which waits for directions of a terminal, and the data flow (**, **-**) read from memory 13 are simplified and shown on the hard configuration of a secure DF card.

[0080] Drawing 12 shows this procedure to the detail, and in drawing 12 , the figure enclosed with an arrow head and a parenthesis shows the procedure after reception typically until the secure DF card A-10 receives <the card control instruction 3> from a terminal A-20.

(H-01): The external communications control means A-14 receives <received data 2> from the A-secure DF card 10 exterior.

(H-02): An external communications control means A-14 by which <received data 2> were received interprets <received data 2> (here, the check of the die length of <received data 2>, reading of an output request J-03, and the check of the termination identifier J-04 are performed from the check of a header J-01, and the part of J-02). Next, the external communications control means A-14 generates <the data receipt 3>, and transmits it to the instruction-execution means A-11.

[0081] (H-03): The instruction-execution means A-11 which received <the data receipt 3> interprets <the data receipt 3> (here, it checks that the check of the die length of <the data receipt 3>, reading of data J-13, and the part of J-14 are "11000111" from the check of the part of J-11 being "01000111", and the part of J-12). Next, the instruction-execution means A-11 generates <the storage control instruction 3>, and transmits it to the storage control means A-12.

(H-04-H-05) The storage control means A-12 which received : <the storage control instruction 3> <The storage control instruction 3> is interpreted (here). It checks that the check of the part of J-51 being "01000011", the check of the die length of the part of J-52 to the <storage control instruction 3>, reading of start-address J-53 and a data length J-54, and the part of J-55 are "11000011." Next, the storage control means A-12 takes out the data specified from the start address J-53 described at <the storage control instruction 3>, and the data length J-54 from the storage means A-13.

[0082] (H-06): The storage control means A-12 generates <the storage control response 3> from the data taken out from the storage means A-13, and transmits it to the instruction-execution means A-11.

(H-07): The instruction-execution means A-11 which received <the storage control response 3> interprets <the storage control response 3> (here, it checks that the check of the part of J-61 being "01000100", the check of the die length of the part of J-62 to the <storage control response 3>, reading of data length J-63 and the body J-64 of data, and the part of D-35 are "11000100"). Next, the instruction-execution means A-11 generates an index J-23 as contents presentation data showing the contents of data from the body J-64 of data.

[0083] (H-08): Next, the instruction-execution means A-11 generates <the data receipt 4> from a data length J-63 and an index J-23, and transmits it to a terminal A-20.

(H-09): An instruction issue means A-21 by which <the data receipt 4> was received interprets <the data receipt 4> (here, it checks that the check of the die length of <the data receipt 4>, reading of index J-23 and a data length J-24, and the part of J-25 are "11001000" from the check of the part of J-21 being "01001000", and the part of J-22). Next, a terminal A-20 displays an index G-23 to the user of a terminal A-20 or the secure DF card A-10, and goes into the waiting state of actuation (propriety of the output from the applicable data storage means A-13 to the exterior) of the degree by the user.

[0084] (H-10): At the terminal A-20 which received the next actuation (the output from the applicable data storage means A-13 to the exterior is possible) from the user, the instruction issue means A-21 publishes <card control instruction 3>, and transmits to the secure DF card A-10.

(H-11): The instruction-execution means A-11 which received <the card control instruction 3> interprets <card control instruction 3> (here, it checks that the check of the die length of <the card control instruction 3>, reading of a data length J-33, and the part of J-34 are "11000001" from the check of the part of J-31 being "01000001", and the part of J-32). Next, the instruction-execution means A-11 generates <the communications control instruction 3> from data length J-33 and the body J-64 of data, and transmits it to the external communications control means A-14. In addition, the instruction-execution means A-11 enciphers the body of data, and you may make it include it in <the communications control instruction 3> at this time.

[0085] (H-12): An external communications control means A-14 by which <the communications control instruction 3> was received interprets <the communications control instruction 3> (here, it checks that the check of the part of J-71 being "01000101", the check of the die length of the part of J-72 to the <communications control instruction 3>, reading of data length J-73 and the body J-74 of data, and the part of J-75 are "11000101"). Next, the external communications control means A-14 outputs the body J-74 of data included in <the communications control instruction 3> from the external communication interface A-16 to the exterior of the secure DF card A-10.

(H-13): After the output to the exterior of the target data is completed, the external communications control means A-14 generates <the communications control response 3>, and transmits it to the instruction-execution means A-11.

[0086] (H-14): The instruction-execution means A-11 which received <the communications control response 3> interprets <the communications control response 3> (here, it checks that the check of the part of J-81 being "01000110", the check of the die length of the part of J-82 to the <communications control response 3>, reading of the processing result J-83, and the part of J-84 are "11000110"). Next, based on the processing result J-83 included in <the communications control response 3>, the instruction-execution means A-11 generates <the card control response 3>, is transmitting to a terminal A-20, and notifies the processing result of <the card control instruction 3> to a terminal A-20.

[0087] (H-15): An instruction issue means A-21 by which <the card control response 3> was received interprets <the card control response 3> (here, it checks that the check of the part of J-41 being "01000010", the check of the die length of the part of J-42 to the <card control

response 3>, reading of the processing result J-43, and the part of J-44 are "11000010"). When the instruction issue means A-21 verifies the contents of this processing result J-43, a terminal A-20 checks the activation result of <the card control instruction 3>.
[0088] in this case, the instruction-execution means A-11 as actuation corresponding to the one <card control instruction 3> which a terminal outputs The actuation which generates <the storage control instruction 3> and reads data from a storage means, Three, the actuation which generates an index J-23 from the body J-64 of data, generates <the data receipt 4>, and is shown to a terminal A-20, and the actuation which generates <the communications control instruction 3> and transmits data outside, are performed. In addition, a format of the above-mentioned instruction is one example, and may use other formats.
[0089] It becomes possible to output the data itself to the A-secure DF card 10 exterior through a terminal A-20, enabling an intention check of a user for the data which it has in the A-storage means 13 interior based on the demand from the outside by making the above processings perform in the A-secure DF card 10 interior.
[0090] For example, when it applies to the dining-room system which deducts the tariff of a card from the configuration of the pan which put this secure DF card on the tray of a dining-room, based on billing inputted from the external communication interface A-16, the screen which checks a user's intention to a terminal is displayed, and when a user consents, the cybermoney equivalent to the claim amount of money is outputted from the external communication interface A-16. In this case, the selection which reduces the pan which the user looked at the claim amount of money, and was put on the tray is also attained.
[0091] In addition, although each operation gestalt explained actuation of the secure DF card which outputs the data stored in the storage means from an external communication interface, or stores in a storage means the data inputted from the external communication interface based on the instruction of a terminal, without minding a terminal When having ordered storing in a storage means the data which the instruction of a terminal outputted the data read from the storage means to the terminal, or inputted from the terminal, according to the instruction, it becomes possible through a terminal to output and input data. That is, it is decided whether to mind a terminal, in case data I/O is carried out with this card, or not mind by whether there is any information meaning what "a terminal is not minded for" in the instruction which an instruction-execution means executes, or there is nothing, and the change can be controlled by description of an instruction.
[0092] The data read from the storage means as structure of a card on the other hand, Or all the data written in a storage means are outputted and inputted, without minding a terminal (that is, even if it does not distinguish "it not minding" "through a terminal" in an instruction). If data are outputted and inputted, without minding a terminal uniformly, it constitutes and it has another way of speaking It is supposed that no read-out/writing from a data storage means by which I/O of the data through a terminal communication interface or the I/O to a terminal communication interface is planned are performed. To a terminal, it can also constitute so that only information other than stereo data used as read-out / write-in object from a storage means, such as data aiming at information presentation besides the index which the instruction-execution means generated at most, or the data for a check at the time of writing, may be sent.
[0093]
[Effect of the Invention] With the secure DF card of this invention, maintenance of the secrecy nature and the integrity of output data is realized to the possibility of unjust actuation of a terminal on the occasion of the output of the data inside a card so that clearly from the above explanation.
[0094] Moreover, even if it faces the input inside [of the data from a card and the terminal outside] a card, maintenance of the secrecy nature and the integrity of input data is realized to the possibility of unjust actuation of a terminal. Moreover, on the occasion of the input inside [of the data from a card and the terminal outside] a card, it becomes possible to a card and a terminal user to urge decision of the validity of data.
[0095] Moreover, on the occasion of the output of the data inside a card based on the trigger from the outside a card and other than a terminal, maintenance of the secrecy nature and the integrity of output data is realized to the possibility of unjust actuation of a terminal.
[0096] Moreover, on the occasion of the output of the data inside a card based on the trigger from the outside a card and other than a terminal, it becomes possible to a card and a terminal user to urge decision of the validity of actuation.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] The hard block diagram of DF card in the operation gestalt of this invention
[Drawing 2] The secure DF card in the operation gestalt of this invention, and the block diagram of a terminal
[Drawing 3] Drawing showing a basic format of the instruction and response in the operation gestalt of this invention
[Drawing 4] Drawing showing the contents of each instruction and response in the 1st operation gestalt of this invention
[Drawing 5] Drawing showing the outline of the output method of the in-house data of the secure DF card in the 1st operation gestalt of this invention
[Drawing 6] Drawing showing the output method of the secure DF card in-house data in the 1st operation gestalt of this invention
[Drawing 7] The example in the case of using the credit card information on DF card in the 1st operation gestalt of this invention
[Drawing 8] Drawing showing the outline of the storing approach of the external data to the secure DF card in the 2nd operation gestalt of this invention
[Drawing 9] Drawing showing the storing approach of the external data to the secure DF card in the 2nd operation gestalt of this invention
[Drawing 10] Drawing showing the contents of the transmitted and received data in the 2nd operation gestalt of this invention, each instruction, and the response
[Drawing 11] Drawing showing the outline of the output method of the secure DF card in-house data in the 3rd operation gestalt of this invention
[Drawing 12] Drawing showing the output method of the secure DF card in-house data in the 3rd operation gestalt of this invention
[Drawing 13] Drawing showing the contents of the transmitted and received data in the 3rd operation gestalt of this invention, each instruction, and the response
[Drawing 14] The hard block diagram of DF card of the conventional technical examples 1-3
[Drawing 15] DF card in the conventional technical examples 1-3, and the block diagram of a terminal
[Drawing 16] Drawing showing the output method of DF card in-house data in the conventional technical example 1
[Drawing 17] Drawing showing the outline of the output method of DF card in-house data in the conventional technical example 1
[Drawing 18] Drawing showing the storing approach of the external data to DF card in the conventional technical example 2
[Drawing 19] Drawing showing the outline of the storing approach of the external data to DF card in the conventional technical example 2
[Drawing 20] Drawing showing the output method of DF card in-house data in the conventional technical example 3
[Drawing 21] Drawing showing the outline of the output method of DF card in-house data in the conventional technical example 3
[Drawing 22] Drawing showing an approach to read the configuration of the IC card in the conventional technical example 4, and a terminal, and a card in-house data
[Description of Notations]
10 Secure DF Card
11 DF Controller
13 Flash Memory
14 DFIO Controller
20 Terminal
30 Card
31 Memory Controller
33 Flash Memory
34 IO Controller
A-10 Secure DF card
A-11 Instruction-execution means
A-12 Storage control means
A-13 Storage means
A-14 External communications control means
A-15 Terminal communication interface
A-16 External communication interface
A-20 Terminal
A-21 Instruction issue means
A-22 Card communication interface
B-01 to B-10 Flow of the instruction, the response, data, and processing in the 1st operation gestalt
C-01 Instruction identifier
C-02 Instruction length
C-03 The contents of an instruction
C-04 Instruction termination identifier
C-11 Response identifier

C-12 Response length
C-13 The contents of a response
C-14 Response termination identifier
D-01 The instruction identifier of <the card control instruction 1>
D-02 Instruction length
D-03 Start address
D-04 Data length
D-05 The instruction termination identifier of <the card control instruction 1>
D-11 The response identifier of <the card control response 1>
D-12 Response length
D-13 Processing result
D-14 The response termination identifier of <the card control response 1>
D-21 The instruction identifier of <the storage control instruction 1>
D-22 Instruction length
D-23 Start address
D-24 Data length
D-25 The instruction termination identifier of <the storage control instruction 1>
D-31 The response identifier of <the storage control response 1>
D-32 Response length
D-33 Data length
D-34 The body of data
D-35 The response termination identifier of <the storage control response 1>
D-41 The instruction identifier of <the communications control instruction 1>
D-42 Instruction length
D-43 Data length
D-44 The body of data
D-45 The instruction termination identifier of <the communications control instruction 1>
D-51 The response identifier of <the communications control response 1>
D-52 Response length
D-53 Processing result
D-54 The response termination identifier of <the communications control response 1>
E-01 to E-10 Flow of the instruction, the response, data, and processing in the 2nd operation gestalt
G-01 The header of <received data 1>
G-02 Received-data length
G-03 The body of data
G-04 The termination identifier of <received data 1>
G-11 The identifier of <the data receipt 1>
G-12 Message length
G-13 Data
G-14 The termination identifier of <the data receipt 1>
G-21 The identifier of <the data receipt 2>
G-22 Message length
G-23 Index
G-24 Body length of data
G-25 The termination identifier of <the data receipt 2>
G-31 The instruction identifier of <the card control instruction 2>
G-32 Instruction length
G-33 Start address
G-34 Data length
G-35 The instruction termination identifier of <the card control instruction 2>
G-41 The response identifier of <the card control response 2>
G-42 Response length
G-43 Processing result
G-44 The response termination identifier of <the card control response 2>
G-51 The instruction identifier of <the storage control instruction 2>
G-52 Instruction length
G-53 Start address
G-54 Data length
G-55 The body of data
G-56 The instruction termination identifier of <the storage control instruction 2>
G-61 The response identifier of <the storage control response 2>
G-62 Response length
G-63 Processing result
G-64 The response termination identifier of <the storage control response 2>
H-01 to H-15 Flow of the instruction, the response, data, and processing in the 3rd operation gestalt
J-01 The header of <received data 2>
J-02 Received-data length
J-03 Output request

J-04 The termination identifier of <received data 2>
J-11 The identifier of <the data receipt 3>
J-12 Message length
J-13 Data
J-14 The termination identifier of <the data receipt 3>
J-21 The identifier of <the data receipt 4>
J-22 Message length
J-23 Index
J-24 Data length
J-25 The termination identifier of <the data receipt 4>
J-31 The instruction identifier of <the card control instruction 3>
J-32 Instruction length
J-33 Data length
J-34 The instruction termination identifier of <the card control instruction 3>
J-41 The response identifier of <the card control response 3>
J-42 Response length
J-43 Processing result
J-44 The response termination identifier of <the card control response 3>
J-51 The instruction identifier of <the storage control instruction 3>
J-52 Instruction length
J-53 Start address
J-54 Data length
J-55 The instruction termination identifier of <the storage control instruction 3>
J-61 The response identifier of <the storage control response 3>
J-62 Response length
J-63 Data length
J-64 The body of data
J-65 The response termination identifier of <the storage control response 3>
J-71 The instruction identifier of <the communications control instruction 3>
J-72 Instruction length
J-73 Data length
J-74 The body of data
J-75 The instruction termination identifier of <the communications control instruction 3>
J-81 The response identifier of <the communications control response 3>
J-82 Response length
J-83 Processing result
J-84 The response termination identifier of <the communications control response 3>
Z-11 Instruction-execution means
Z-12 Storage control means
Z-13 Storage means
Z-14 External communications control means
Z-15 Terminal communication interface
Z-16 External communication interface
Z-21 Instruction issue means
Z-22 Card communication interface
Y-01 to Y-05 Flow of the instruction, the response, data, and processing in the conventional technical example 1
X-01 to X-06 Flow of the instruction, the response, data, and processing in the conventional technical example 2
W-01 to W-06 Flow of the instruction, the response, data, and processing in the conventional technical example 3
V-01 to V-04 Flow of the instruction, the response, data, and processing in the conventional technical example 4
V-11 Instruction-execution means
V-12 Storage control means
V-13 Storage means
V-14 Terminal communication interface
V-21 Instruction issue means
V-22 Card communication interface

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－196624
（P2003－196624A）
(43)公開日　平成15年７月11日(2003.7.11)

(51)Int.Cl.'	識別記号	FI		テーマコード（参考）
G06K 19/07		B42D 15/10	521	2C005
B42D 15/10	521	G06F 3/08	C	5B035
G06F 3/08		G06K 19/00	N	5B065
G06K 19/073			P	

審査請求　未請求　請求項の数28　ＯＬ　（全 21 頁）

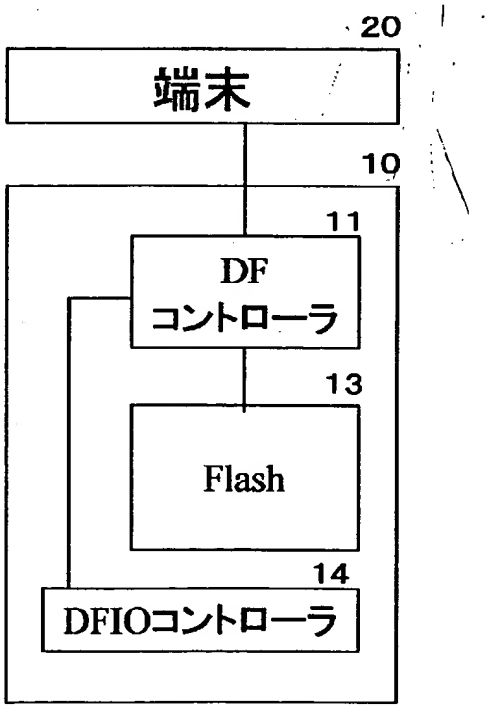
(21)出願番号　特願2001－397292(P2001－397292)
(22)出願日　平成13年12月27日(2001.12.27)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　佐々木　理
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　中西　良明
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100099254
弁理士　役　昌明　（外３名）

最終頁に続く

(54)【発明の名称】　デュアルファンクションカード

(57)【要約】
【課題】　端末による不正動作が介入する余地を排除し、外部からのデータの不正な書き込みや読み出しを防ぎ、蓄積データの秘匿性・完全性を保持することができるＤＦカードを提供する。
【解決手段】　端末20との端末通信インタフェースと、外部との外部通信インタフェースと、データの記憶手段13とを内蔵するＤＦカード10において、端末から受信した命令を実行する命令実行手段11と、命令実行手段の命令を受けて記憶手段へのデータの書き込み及び読み出しを制御する記憶制御手段11と、命令実行手段の命令を受けて外部通信インタフェースからの通信データの入出力を制御する外部通信制御手段14とを設けている。端末の指示のもとに、内部データを端末を介さずに外部に出力し、外部データを端末を介さずに格納するようにしているため、端末による不正動作を防止し、カード内部データの秘匿性・完全性を保持することができる。



1

【特許請求の範囲】

【請求項１】　端末との端末通信インタフェースと、外部との外部通信インタフェースと、データの記憶手段とを内蔵するデュアルファンクションカードであって、前記端末通信インタフェースまたは外部通信インタフェースから受信した命令を実行する命令実行手段と、前記命令実行手段の命令を受けて前記記憶手段へのデータの書き込み及び読み出しを制御する記憶制御手段と、前記命令実行手段の命令を受けて前記外部通信インタフェースからの通信データの入出力を制御する外部通信制御手段とを備えることを特徴とするデュアルファンクションカード。

【請求項２】　前記記憶制御手段及び外部通信制御手段が前記命令実行手段の命令のみを受けて動作することを特徴とする請求項１に記載のデュアルファンクションカード。

【請求項３】　前記命令実行手段及び記憶制御手段が、耐タンパーＩＣチップ上にソフトウェアとして実装されていることを特徴とする請求項１に記載のデュアルファンクションカード。

【請求項４】　前記外部通信制御手段が、前記命令実行手段及び記憶制御手段とともに、耐タンパーＩＣチップ上にソフトウェアとして実装されていることを特徴とする請求項３に記載のデュアルファンクションカード。

【請求項５】　前記命令実行手段が、耐タンパーＩＣチップ上にソフトウェアとして実装され、前記記憶制御手段及び外部通信制御手段が、各々耐タンパー性のハードウェアとして実装されていることを特徴とする請求項１に記載のデュアルファンクションカード。

【請求項６】　前記命令実行手段が、前記記憶制御手段を通じて前記記憶手段から読み出したデータを、前記外部通信制御手段を通じて前記外部通信インタフェースから出力することを特徴とする請求項１に記載のデュアルファンクションカード。

【請求項７】　前記命令実行手段は、端末から、前記記憶手段で格納するデータを端末を介さずに外部に出力する命令を受けて、前記記憶制御手段を通じて前記記憶手段からデータを読み出す動作と、前記外部通信制御手段を通じて前記データを前記外部通信インタフェースから出力する動作とを行うことを特徴とする請求項１に記載のデュアルファンクションカード。

【請求項８】　前記命令実行手段が、前記外部通信インタフェースから入力したデータの内容を端末に提示することを特徴とする請求項１に記載のデュアルファンクションカード。

【請求項９】　前記命令実行手段は、前記データの内容を表す内容提示データを作成し、前記内容提示データを端末に提示することを特徴とする請求項８に記載のデュアルファンクションカード。

【請求項１０】　前記命令実行手段は、前記端末の指示を受けて、前記外部通信インタフェースから入力した前記データを前記記憶制御手段を通じて前記記憶手段に格納することを特徴とする請求項８または９に記載のデュアルファンクションカード。

【請求項１１】　前記命令実行手段は、前記外部通信インタフェースからデータが入力したとき、前記データの内容を表す内容提示データを作成して端末に提示する動作と、端末から、前記外部通信インタフェースで受信したデータを、端末を介さずに前記記憶手段に格納する命令を受けて、前記記憶制御手段を通じて前記データを前記記憶手段へ格納する動作とを行うことを特徴とする請求項１に記載のデュアルファンクションカード。

【請求項１２】　前記命令実行手段が、前記記憶制御手段を通じて前記記憶手段から読み出したデータの内容を表す内容提示データを作成して端末に提示することを特徴とする請求項１に記載のデュアルファンクションカード。

【請求項１３】　前記命令実行手段は、前記外部通信インタフェースを通じて外部からデータの要求があったとき、該当するデータの内容を表す内容提示データを作成して端末に提示することを特徴とする請求項１２に記載のデュアルファンクションカード。

【請求項１４】　前記命令実行手段は、前記端末の指示を受けて、前記データを前記外部通信制御手段を通じて前記外部通信インタフェースから出力することを特徴とする請求項１３に記載のデュアルファンクションカード。

【請求項１５】　前記命令実行手段が、前記外部通信制御手段を通じて出力する前記データを暗号化することを特徴とする請求項６または請求項１４に記載のデュアルファンクションカード。

【請求項１６】　前記命令実行手段は、前記外部通信インタフェースからデータ要求が入力したとき、要求されたデータを前記記憶制御手段を通じて前記記憶手段から読み出す動作と、前記データの内容を表す内容提示データを作成して端末に提示する動作と、端末から、外部のデータ要求に応えて前記記憶手段に格納されたデータを、端末を介さずに外部に出力する命令を受けて、前記データを前記外部通信制御手段を通じて前記外部通信インタフェースから出力する動作とを行うことを特徴とする請求項１に記載のデュアルファンクションカード。

【請求項１７】　前記命令実行手段または記憶手段は、前記端末通信インタフェースから入力されるデータは前記記憶手段に格納しないこと、または／及び、前記記憶手段から読み出されるデータは前記端末通信インタフェースへ送出しないことを特徴とする請求項１に記載のデュアルファンクションカード。

【請求項１８】　端末との端末通信インタフェースと、外部との外部通信インタフェースと、データの記憶手段とを内蔵するデュアルファンクションカードに対して端

2

末から出される命令であって、前記記憶手段で保持するデータを端末を介さずに外部に出力することを指示する命令。

【請求項19】　端末との端末通信インタフェースと、外部との外部通信インタフェースと、データの記憶手段とを内蔵するデュアルファンクションカードに対して端末から出される命令であって、前記外部通信インタフェースで受信したデータを、端末を介さずに前記記憶手段に格納することを指示する命令。

【請求項20】　端末との端末通信インタフェースと、外部との外部通信インタフェースと、データの記憶手段とを内蔵するデュアルファンクションカードに対して端末から出される命令であって、前記外部通信インタフェースから入力するデータ要求に応えて前記記憶手段に格納されたデータを、端末を介さずに外部に出力することを指示する命令。

【請求項21】　端末との端末通信インタフェースと、外部との外部通信インタフェースと、データの記憶手段とを内蔵するデュアルファンクションカードに対して端末から出される命令であって、1つの命令に基づいてデュアルファンクションカードに複数の動作を行わせることを特徴とする命令。

【請求項22】　端末との端末通信インタフェースと、外部との外部通信インタフェースと、データの記憶手段とを内蔵するデュアルファンクションカードの内部データの出力方法であって、端末からのデータ出力指示を受けて、前記記憶手段に格納されたデータを前記端末を介さずに外部に出力することを特徴とするデータ出力方法。

【請求項23】　端末から、前記記憶手段で格納するデータを端末を介さずに外部に出力する命令を受けて、前記記憶手段からデータを読み出す動作と、前記データを前記外部通信インタフェースから出力する動作とを行うことを特徴とする請求項22に記載のデータ出力方法。

【請求項24】　端末との端末通信インタフェースと、外部との外部通信インタフェースと、データの記憶手段とを内蔵するデュアルファンクションカードの外部データの格納方法であって、前記外部通信インタフェースから入力するデータの内容を表す内容提示データを端末に提示し、端末からの格納指示を受けて、前記記憶手段に格納するデータを前記端末を介さずに格納することを特徴とするデータ格納方法。

【請求項25】　前記外部通信インタフェースからデータが入力したとき、前記内容提示データを作成して端末に提示する動作と、端末から、前記外部通信インタフェースで受信したデータを、端末を介さずに前記記憶手段に格納する命令を受けて、前記データを前記記憶手段へ格納する動作とを行うことを特徴とする請求項24に記載データ格納方法。

【請求項26】　端末との端末通信インタフェースと、

外部との外部通信インタフェースと、データの記憶手段とを内蔵するデュアルファンクションカードの内部データの出力方法であって、前記外部通信インタフェースから前記記憶手段に格納されたデータのデータ要求が入力されたとき、該当するデータの内容を表す内容提示データを端末に提示し、端末からのデータ出力指示を受けて、前記データを前記端末を介さずに外部に出力することを特徴とするデータ出力方法。

【請求項27】　前記外部通信インタフェースからデータ要求が入力したとき、要求されたデータを前記記憶手段から読み出す動作と、前記内容提示データを作成して端末に提示する動作と、端末から、外部のデータ要求に応えて前記記憶手段に格納されたデータを、端末を介さずに外部に出力する命令を受けて、前記データを前記外部通信インタフェースから出力する動作とを行うことを特徴とする請求項26に記載のデータ出力方法。

【請求項28】　前記データを暗号化して外部に出力することを特徴とする請求項22または26に記載のデータ出力方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、メモリカードに関し、特に、データを記憶するメモリと、端末との接点以外に外部通信インタフェースを持つ、デュアルファンクションカードの構成に関するものである。

【0002】

【従来の技術】（従来技術例1）近年、ICカードは、定期券やテレホンカード、キャッシュカードなどに利用され、メモリカードは、PC（パーソナルコンピュータ）やデジタルカメラ、音楽プレーヤーの記憶媒体などに利用されるなど、双方とも多方面で利用されている。メモリカードはデジタルカメラや音楽プレーヤーなどの内蔵記憶領域を補うことと、可搬性を目的として利用されている。例えば、デジタルカメラで撮影した画像データを、装着しているメモリカードに記憶し、このメモリカードをPCに装着することで、PC上で前記画像の閲覧が可能になる。端末以外との外部通信インタフェースを持つインタフェースカードは、PCMCIA規格でPCと接続され、モデムカード・LANカードなどとして使用される。これにより、モデム・LANなどの機能を内蔵しないPCにおいても、外部とのデータ通信が可能となる。

【0003】メモリと外部通信インタフェースとを内蔵する従来のデュアルファンクションカード（以下、DFカードと言う）は、ハード構成として、図14に示すように、データを記憶するフラッシュメモリ33と、端末20からの指示に従ってフラッシュメモリ33のデータの読み出し／書き込みを制御するメモリコントローラ31と、端末20からの指示に従って外部へのデータの入出力を制御するIOコントローラ34とを備えている。このDFカー

ド30の機能ブロックは、図１５に示すように、端末との通信を行う端末通信インタフェースZ-15、端末から受信した命令を実行する命令実行手段Z-11、データを保持する記憶手段Z-13、記憶手段Z-13へのデータの読み出し／書き込みを行う記憶制御手段Z-12、端末以外のカード外部デバイスとのデータ通信を行う外部通信インタフェースZ-16、外部通信インタフェースへの通信データの読み出し／書き込みを行う外部通信制御手段Z-14とから構成される。

【０００４】このうち、命令実行手段Z-11及び記憶制御手段Z-12はメモリコントローラ31が有する機能であり、また、記憶手段Z-13はフラッシュメモリ33に、外部通信制御手段Z-14はＩＯコントローラ34に対応している。まず、このＤＦカードにおいて、記憶手段Z-13内に保持するデータを外部通信インタフェースZ-16から出力しようとした場合、図１６（Y-01）～（Y-05）の矢印で示した順序に従う。

（Y-01）：端末の命令発行手段Z-21が命令を発行し、ＤＦカードに送信する。

（Y-02）・（Y-03）：端末からの命令を受信した命令実行手段Z-11が、記憶制御手段Z-12に処理を要求し、記憶手段Z-13からデータを取り出す。

（Y-04）：命令実行手段Z-11は、端末からの命令に対する返答として、記憶手段Z-13から取り出したデータを端末に送信する。

（Y-05）：命令発行手段Z-21が、ＤＦカードから受信したデータを外部通信制御手段Z-14からカード外部に出力する。

また、図１７は、ハード構成上において、メモリまでの指示の流れ（①～②）と、メモリから読み出されたデータの流れ（③～⑥）とを示している。以上のように、ＤＦカード内部のデータをカード外部に出力したい場合、該当するデータは一旦カード内部から端末に取り出されなければならない。

【０００５】（従来技術例２）また、このＤＦカードにおいて、外部通信インタフェースZ-16から受信したデータを記憶手段Z-13に格納しようとした場合、図１８（X-01）～（X-06）の矢印で示した順序に従う。

（X-01）：ＤＦカードの外部通信制御手段Z-14が、外部からのデータを受信する。

（X-02）：外部通信制御手段Z-14が、端末に対して受信データを送信する。

（X-03）：命令発行手段Z-21によりＤＦカードからデータを受信した端末が、受信データを端末やＤＦカードのユーザに対して表示し、ユーザによる次の操作（受信データの記憶手段Z-13への格納の可否）の待ち状態に入る。

（X-04）：ユーザから次の操作（受信データの記憶手段Z-13への格納可）を受けた端末は、命令発行手段Z-21が命令を発行し、ＤＦカードに送信する。なお、ここでの命令は、内部にＤＦカードからの受信データを含んでいる。

（X-05）：端末からの命令を受信した命令実行手段Z-11が、記憶制御手段Z-12に処理を要求し、命令内部に含まれている、ＤＦカード外部からの受信データを記憶手段Z-13に格納する。

（X-06）：命令実行手段Z-11が、端末からの命令に対する返答として、データ格納処理の結果を送信する。

なお、（X-03）・（X-04）において、端末やＤＦカードのユーザに対して、次の動作を実行するための操作権限を与えずに、すべて自動で行う場合も有り得る。また、図１９は、　ハード構成上において、メモリまでの指示及びデータの流れ（①～④）を示している。このときのハード構成上でのデータの流れ（①～④）を示している。

【０００６】以上のように、ＤＦカード外部からカード内部にデータを格納したい場合、外部から受信したデータは一旦端末を経由しなければならない。また、（X-03）・（X-04）において上記のようにすべて自動化した場合、端末やＤＦカードのユーザが格納を望まないデータを、カード内部に格納することが可能となってしまう。

【０００７】（従来技術例３）また、このＤＦカードにおいて、端末ではない外部からの要求により、記憶手段Z-13内に保持するデータを外部通信インタフェースZ-16から出力しようとした場合、図２０（W-01）～（W-06）の矢印で示した順序に従う。

（W-01）：外部通信制御手段Z-14が、ＤＦカード外部から要求通知を受信する。

（W-02）：外部通信制御手段Z-14は、要求通知を端末に送信する。

（W-03）：要求通知を受信した命令発行手段Z-21は、該当データを出力するための命令を発行し、ＤＦカードに送信する。

（W-04・W-05）：端末からの命令を受信した命令実行手段Z-11は、記憶制御手段Z-12に処理を要求し、記憶手段Z-13からデータを取り出す。

（W-06）：命令実行手段Z-11は、端末からの命令に対する返答として、記憶手段Z-13から取り出したデータを端末に送信する。

（W-07）：命令発行手段Z-21が、ＤＦカードから受信したデータを外部通信制御手段Z-14からカード外部に出力する。

【０００８】なお、（W-03）において、端末やＤＦカードのユーザに対して、次の動作実行への操作を促す場合も有り得る。また、図２１は、ハード構成上において、メモリまでの指示の流れ（①～④）と、メモリから読み出されたデータの流れ（⑤～⑧）とを示している。以上のように、ＤＦカード外部からの要求によりカード内部のデータを出力したい場合も、該当データは一旦端末を

経由しなければならない。さらに、端末やＤＦカードのユーザが望まないデータを、カード外部に出力することも可能になってしまう。

【０００９】（従来技術例４）次に、従来のＩＣカード（接触インタフェースか、非接触インタフェースかはここでは問わない）において、カード内部のデータを端末に取り出す場合について説明する。図２２に示すようにＩＣカードは、端末との通信を行う端末通信インタフェースV-14、端末から受信した命令を実行する命令実行手段V-11、データを保持する記憶手段V-13、記憶手段Z-13へのデータの読み出し／書き込みを行う記憶制御手段V-12とから構成される。このＩＣカードにおいて、記憶手段V-13内に保持するデータを端末が読み出そうとした場合、図２２（V-01）～（V-04）の矢印で示した順序に従う。

（V-01）：端末の命令発行手段V-21が命令を発行し、ＩＣカードに送信する。

（V-02）・（V-03）：端末からの命令を受信した命令実行手段V-11が、記憶制御手段V-12に処理を要求し、記憶手段V-13からデータを取り出す。

（V-04）：命令実行手段V-11は、端末からの命令に対する返答として、記憶手段V-13から取り出したデータを端末に送信する。

以上のように、ＩＣカード内部のデータを端末に取り出す場合、一旦端末により命令が発行されると、処理終了まではカードユーザによる、取り出すデータの内容の把握や、操作（データの読み出し）の中断などの判断はできない。

【００１０】

【発明が解決しようとする課題】（従来技術例１）におけるＤＦカードの場合、記憶手段Z-13内のデータを一旦端末に渡してからでないと外部に出力できないため、重要なデータ（例えば、クレジットカード番号や電子マネー等）を扱う場合には、端末が不正な動作をしないことが保証されていなければならない。ここでの端末の不正な動作とは、データの不正な改ざん・蓄積・削除などが挙げられる。

【００１１】また、（従来技術例２）におけるＤＦカードの場合も、カード外部からの受信データを一旦端末に渡してからでないと外部に出力できないため、（従来技術例１）におけるものと同様の課題が挙げられる。さらに、端末やＤＦカードのユーザが望まないデータを、カード内部に格納されてしまう危険がある。

【００１２】同様に、（従来技術例３）におけるＤＦカードの場合も、カード外部からの要求及び記憶手段Z-13内のデータの双方を一旦端末に渡さなければならないため、（従来技術例１）におけるものと同様の課題が挙げられる。さらに、端末やＤＦカードのユーザが望まないデータをカード外部に出力されてしまう危険がある。また、（従来技術例４）におけるＩＣカードの場合、端末が発行した命令によりどのデータが取り出されるのかが、処理終了までカードユーザには分からないため、端末が不正な動作をしないことが保証されていなければならない。

【００１３】本発明は、こうした課題を解決するものであり、端末による不正動作が介入する余地を排除し、また、外部からのデータの不正な書き込みや読み出しを防ぎ、蓄積データの秘匿性・完全性を保持することができるＤＦカードを提供し、また、このＤＦカードのデータ出力方法及びデータ格納方法を提供することを目的としている。

【００１４】

【課題を解決するための手段】そこで、本発明では、端末との端末通信インタフェースと、外部との外部通信インタフェースと、データの記憶手段とを内蔵するＤＦカードにおいて、端末通信インタフェースまたは外部通信インタフェースから受信した命令を実行する命令実行手段と、命令実行手段の命令を受けて記憶手段へのデータの書き込み及び読み出しを制御する記憶制御手段と、命令実行手段の命令を受けて外部通信インタフェースからの通信データの入出力を制御する外部通信制御手段とを設けている。

【００１５】また、このＤＦカードのデータ出力方法において、端末からのデータ出力指示を受けて、記憶手段に格納されたデータを端末を介さずに外部に出力するようにしている。また、このＤＦカードのデータ格納方法において、外部通信インタフェースから入力するデータの内容を表す内容提示データを端末に提示し、端末からの格納指示を受けて、記憶手段に格納するデータを端末を介さずに格納するようにしている。また、このＤＦカードのデータ出力方法において、外部通信インタフェースから記憶手段に格納されたデータのデータ要求が入力されたとき、該当するデータの内容を表す内容提示データを端末に提示し、端末からのデータ出力指示を受けて、このデータを端末を介さずに外部に出力するようにしている。

【００１６】これにより、端末による不正動作を防止したＤＦカードを構成することができ、カード内部データの秘匿性・完全性を保持することができる。また、ＤＦカード内部に保存されているデータを、端末を介さずに外部に出力することにより、出力データの秘匿性・完全性が保持される。また、入力データを、端末を介さずにＤＦカード内部に保存することにより、入力データの秘匿性・完全性が保持される。また、ＤＦカード・端末以外の外部からの入力をトリガーとして、ＤＦカード内部に保存されているデータを、端末を介さずに外部に出力することにより、出力データの秘匿性・完全性が保持される。

【００１７】

【発明の実施の形態】（第１の実施形態）第１の実施形

態では、本発明におけるセキュアＤＦカードの全体構成と動作について説明する。本発明の実施形態におけるセキュアＤＦカードは、ハード構成として、図１に示すように、データを記憶するフラッシュメモリ13と、外部とのデータの入出力を制御するＤＦＩＯコントローラ14と、端末20からの指示を受けてフラッシュメモリ13のデータの読み出し／書き込み、及び、ＤＦＩＯコントローラ14のデータ入出力動作を制御するＤＦコントローラ11とを備えている。

【００１８】このＤＦカードは、機能的には、図２に示すように、端末A-20とのデータ通信を行う端末通信インタフェースA-15、端末A-20から受信した命令を実行する命令実行手段A-11、データを保持する記憶手段A-13、記憶手段A-13へのデータの読み出し／書き込みを行う記憶制御手段A-12、端末A-20以外のカード外部デバイスとのデータ通信を行う外部通信インタフェースA-16、外部通信インタフェースA-16への通信データの読み出し／書き込みを行う外部通信制御手段A-14とから構成される。このうち、命令実行手段A-11及び記憶制御手段A-12はＤＦコントローラ11が有する機能であり、また、記憶手段A-13はフラッシュメモリ13に、外部通信制御手段A-14はＤＦＩＯコントローラ14に対応している。

【００１９】この命令実行手段A-11及び記憶制御手段A-12は、それぞれを、ソフトウェアモジュールとして１つのＩＣチップ内部に構成し、ハードウェア的に耐タンパー性を持たせる。こうすることにより、記憶手段A-13が、耐タンパー性を持たないフラッシュメモリであっても、記憶手段A-13に書き込むデータを命令実行手段A-11で暗号化することにより、記憶手段A-13に書き込むデータの秘匿性を保持することができる。

【００２０】また、命令実行手段A-11及び記憶制御手段A-12をＩＣ化するとき、外部通信制御手段A-14もソフトウェアモジュールとして同じＩＣチップ内部に構成してもよい。この場合、命令実行手段A-11、記憶制御手段A-12及び外部通信制御手段A-14を、ハードウェア的に耐タンパー性を持つ１つのＩＣチップとして構成することができる。また、命令実行手段A-11、記憶制御手段A-12及び外部通信制御手段A-14の各々をハードウェアとして、耐タンパー性を持つ１つのチップ内部に構成しても良い。また、命令実行手段A-11は耐タンパー性ＩＣチップ上にソフトウェアとして構成し、記憶制御手段A-12及び外部通信制御手段A-14はハードウェアとして実装して耐タンパー性を持たせるようにしても良い。この構成を採ることにより、従来のカードで使われていた記憶制御手段及び外部通信制御手段を構成するハードウェアを、本発明のセキュアＤＦカードに転用することができる。

【００２１】このセキュアＤＦカードにおいて、命令実行手段A-11は、命令発行手段A-21が発行したカード制御命令を解釈し、その内容によって記憶制御手段A-12や外部通信制御手段A-14に対して、処理を要求する。また、カード制御命令に対するカード制御応答を、端末A-20に対して返す。記憶制御手段A-12は、命令実行手段A-11からの処理要求に基づき、記憶手段A-13内部の指定された領域に対して、データの読み出し／書き込みを行う。

【００２２】外部通信制御手段A-14は、命令実行手段A-11からの処理要求に基づき、指定されたデータを外部通信インタフェースA-16に出力、あるいは外部通信インタフェースA-16に受信したデータを命令実行手段A-11に入力する。端末通信インタフェースA-15は、端末A-20のカード通信インタフェースA-22との接点を持ち、端末A-20とセキュアＤＦカードA-10間でのシリアル通信を行う。外部通信インタフェースA-16は、外部通信制御手段A-14の制御に従い、端末A-20以外の外部デバイスとのデータ通信を行う。このインタフェースは、赤外線・Bluetooth・ISO14443などの無線通信規格や、IEEE1394・USBなどの有線通信規格に対応し、外部通信制御手段A-14は、外部通信インタフェースA-16が対応する通信規格に基づき制御するためのモジュールとなっている。

【００２３】また、本発明の実施形態における端末A-20は、図２に示すように、セキュアＤＦカードA-10とのデータ通信を行うカード通信インタフェースA-22と、セキュアＤＦカードA-10へのカード制御命令を発行する命令発行手段A-21とから構成される。この端末A-20は、例えば、パーソナルコンピュータや、携帯電話、テレビのリモコン等である。セキュアＤＦカードA-10は、端末A-20の命令発行手段A-21が発行したカード制御命令を、カード通信インタフェースA-22、端末通信インタフェースA-15を介して受信し、その命令を命令実行手段A-11が実行することにより、動作する。

【００２４】ここでは、命令発行手段A-21が発行するカード制御命令は、

＜カード制御命令１＞記憶手段A-13が保持するデータを、端末A-20を介さずに外部通信インタフェースA-16から外部へ出力する

＜カード制御命令２＞外部通信インタフェースA-16により外部から受信したデータを、端末A-20を介さずに記憶手段A-13へ入力する

＜カード制御命令３＞端末A-20以外のセキュアＤＦカードA-10外部からの要求により、記憶手段A-13が保持するデータを、端末A-20を介さずに外部通信インタフェースA-16から外部へ出力する

の３種類であるとする。

【００２５】以下で、セキュアＤＦカードA-10が＜カード制御命令１＞を受信した場合の動作について、詳細を説明する。図３において、命令発行手段A-21・命令実行手段A-11が発行する命令の基本フォーマットを（Ａ）に、命令実行手段A-11・記憶制御手段A-12・外部通信制御手段A-14が発行する応答の基本フォーマットを（Ｂ）に示している。図３（Ａ）において、命令識別子C-01は命令の種類、命令長C-02は命令のデータ長、命令内容C-

03はその命令の実行に必要なデータ、命令終了識別子C-04はその命令が終了することを表す識別子をそれぞれ表している。また図3（B）において、応答識別子C-11は応答の種類、応答長C-12は応答のデータ長、応答内容C-13は命令に対する実行結果を表すデータ、応答終了識別子C-14はその応答が終了することを表す識別子をそれぞれ表している。

【0026】次に図4に、本実施形態における＜命令1＞及び、それに対する＜応答1＞の構造をそれぞれ、（A）～（F）に示す。図4（A）は、命令発行手段A-21が発行する＜カード制御命令1＞を表している。D-01は命令識別子C-01に対応し、＜カード制御命令1＞では“00001001”となる。D-02は命令長C-02に対応し、＜カード制御命令1＞の長さを示す。先頭アドレスD-03・データ長D-04は命令内容C-03に対応している。先頭アドレスD-03は、＜カード制御命令1＞により、記憶手段A-13内部に保持されている、外部通信インタフェースA-16から出力するデータの先頭アドレス（論理アドレス）を示す。データ長D-04は、記憶手段A-13内部に保持されている、外部通信インタフェースA-16から出力するデータの長さを示す。D-05は命令終了識別子C-04に対応し、＜カード制御命令1＞では“10001001”となる。

【0027】図4（B）は、命令実行手段A-11が発行する＜カード制御応答1＞を表している。D-11は応答識別子C-11に対応し、＜カード制御応答1＞では“00001010”となる。D-12は応答長C-12に対応し、＜カード制御応答1＞の長さを示す。処理結果D-13は応答内容C-13に対応し、＜カード制御命令1＞の実行結果の成功（“00000000”）または失敗（“11111111”）を示す数列が入る。D-14は応答終了識別子C-14に対応し、＜カード制御応答1＞では“10001010”となる。

【0028】図4（C）は、命令実行手段A-11が発行する＜記憶制御命令1＞を表している。D-21は命令識別子C-01に対応し、＜記憶制御命令1＞では“00001011”となる。D-22は命令長C-02に対応し、＜記憶制御命令1＞の長さを示す。先頭アドレスD-23・データ長D-24は命令内容C-03に対応している。先頭アドレスD-23・データ長D-24が持つ意味は、＜カード制御命令1＞における先頭アドレスD-03・データ長D-04と同様である。D-25は命令終了識別子C-04に対応し、＜記憶制御命令1＞では“10001011”となる。

【0029】図4（D）は、記憶制御手段A-12が発行する＜記憶制御応答1＞を表している。D-31は応答識別子C-11に対応し、＜記憶制御応答1＞では“00001100”となる。D-32は応答長C-12に対応し、＜記憶制御応答1＞の長さを示す。データ長D-33・データ本体D-34は応答内容C-13に対応している。データ長D-33は、後に続くデータ本体D-34の長さを示す。データ本体D-34は、＜記憶制御命令1＞により指定され、記憶手段A-13から取り出されたデータの本体が入る。D-35は応答終了識別子C-14に対応し、＜記憶制御応答1＞では“10001100”となる。

【0030】図4（E）は、命令実行手段A-11が発行する＜通信制御命令1＞を表している。D-41は命令識別子C-01に対応し、＜通信制御命令1＞では“00001101”となる。D-42は命令長C-02に対応し、＜通信制御命令1＞の長さを示す。データ長D-43・データ本体D-44は命令内容C-03に対応している。データ長D-43・データ本体D-44が持つ意味は、＜記憶制御応答1＞におけるデータ長D-33・データ本体D-34と同様である。D-45は命令終了識別子C-04に対応し、＜通信制御命令1＞では“10001101”となる。

【0031】図4（F）は、外部通信制御手段A-14が発行する＜通信制御応答1＞を表している。D-51は応答識別子C-11に対応し、＜通信制御応答1＞では“00001110”となる。D-52は応答長C-12に対応し、＜通信制御応答1＞の長さを示す。処理結果D-53は応答内容C-13に対応し、＜通信制御命令1＞の実行結果の成功（“00000000”）または失敗（“11111111”）を示す数列が入る。D-54は応答終了識別子C-14に対応し、＜通信制御応答1＞では“10001110”となる。

【0032】次に、セキュアＤＦカードA-10内部での動作について説明する。図5は、端末20からの指示に基づいて、セキュアＤＦカード10のメモリ13で保持されたデータを外部に出力する場合のメモリ13への指示の流れ（①～②）と、メモリ13から読み出されたデータの流れ（③～⑤）とをセキュアＤＦカードのハード構成上に簡略化して示している。

【0033】図6は、この詳細を示している。図6において、矢印と括弧で囲んだ数字は、セキュアＤＦカードA-10が端末A-20から＜カード制御命令1＞を受信した場合の処理手順を模式的に示している。　（B-01）：端末A-20の命令発行手段A-21が＜カード制御命令1＞を発行し、セキュアＤＦカードA-10に送信する。

【0034】（B-02）：＜カード制御命令1＞を受信したセキュアＤＦカードA-10の命令実行手段A-11は、＜カード制御命令1＞の解釈を行う（ここでは、D-01の部分が“00001001”であることの確認、D-02の部分から＜カード制御命令1＞の長さの確認、先頭アドレスD-03・データ長D-04の読み取り、D-05の部分が“10001001”であることの確認、を行う）。次に命令実行手段A-11は、＜記憶制御命令1＞を生成し、記憶制御手段A-12に送信する。

【0035】（B-03・B-04）：＜記憶制御命令1＞を受信した記憶制御手段A-12は、＜記憶制御命令1＞の解釈を行う（ここでは、D-21の部分が“00001011”であることの確認、D-22の部分から＜記憶制御命令1＞の長さの確認、先頭アドレスD-23・データ長D-24の読み取り、D-25の部分が“10001011”であることの確認、を行う）。次に記憶制御手段A-12は、＜記憶制御命令1＞に記された先頭アドレスD-23とデータ長D-24とから、指定された

データを記憶手段A-13から取り出す。

【００３６】（B-05）：記憶制御手段A-12は、記憶手段A-13から取り出したデータから＜記憶制御応答１＞を生成し、命令実行手段A-11に送信する。

（B-06）：＜記憶制御応答１＞を受信した命令実行手段A-11は、＜記憶制御応答１＞の解釈を行う（ここでは、D-31の部分が“00001100”であることの確認、D-32の部分から＜記憶制御応答１＞の長さの確認、データ長D-33・データ本体D-34の読み取り、D-35の部分が“10001100”であることの確認、を行う）。次に命令実行手段A-11は、データ長D-33・データ本体D-34から＜通信制御命令１＞を生成し、外部通信制御手段A-14に送信する。なお、このとき、命令実行手段A-11は、データ本体D-44を暗号化して＜通信制御命令１＞の中に含めるようにしても良い。

【００３７】（B-07）：＜通信制御命令１＞を受信した外部通信制御手段A-14は、＜通信制御命令１＞の解釈を行う（ここでは、D-41の部分が“00001101”であることの確認、D-42の部分から＜通信制御命令１＞の長さの確認、データ長D-43・データ本体D-44の読み取り、D-45の部分が“10001101”であることの確認、を行う）。次に外部通信制御手段A-14は、＜通信制御命令１＞内に含まれる、データ本体D-44を、外部通信インタフェースA-16からセキュアＤＦカードA-10の外部に出力する。なお、命令実行手段A-11によりデータ本体D-44が暗号化されている場合、その復号化は、このデータ本体D-44を受信した先で行われる。

【００３８】（B-08）：目的のデータの外部への出力が終了すると、外部通信制御手段A-14は＜通信制御応答１＞を生成し、命令実行手段A-11に送信する。

（B-09）：＜通信制御応答１＞を受信した命令実行手段A-11は、＜通信制御応答１＞の解釈を行う（ここでは、D-51の部分が“00001110”であることの確認、D-52の部分から＜通信制御応答１＞の長さの確認、処理結果D-53の読み取り、D-54の部分が“10001110”であることの確認、を行う）。次に命令実行手段A-11は、＜通信制御応答１＞内に含まれる、処理結果D-53に基づき、＜カード制御応答１＞を生成し、端末A-20に送信することで、＜カード制御命令１＞の処理結果を端末A-20に対して通知する。

【００３９】（B-10）：＜カード制御応答１＞を受信した命令発行手段A-21は、＜カード制御応答１＞の解釈を行う（ここでは、D-11の部分が“00001010”であることの確認、D-12の部分から＜カード制御応答１＞の長さの確認、処理結果D-13の読み取り、D-14の部分が“10001010”であることの確認、を行う）。この処理結果D-13の内容を命令発行手段A-21が検証することにより、端末A-20は＜カード制御命令１＞の実行結果を確認する。

【００４０】ここで注目すべき点は、このセキュアＤＦカードA-10の命令実行手段A-11が、端末A-20の命令発行手段A-21から一つの命令を受けて、複数の動作を実行することである。即ち、端末A-20の命令発行手段A-21から＜カード制御命令１＞を受信すると、＜記憶制御命令１＞を生成して記憶手段A-13からデータを読み出し、また、＜通信制御命令１＞を生成して外部通信インタフェースA-16から外部にデータを出力している。

【００４１】受動的に動作する従来のカードでは、一つの命令を受けると、一つの動作のみを行うのが通常であるが、このセキュアＤＦカードA-10の命令実行手段A-11は、一命令に対して複数の動作を行っており、それにより、記憶手段A-13内部に持つデータを、端末A-20を仲介せずにセキュアＤＦカードA-10外部に出力することが可能になる。なお、前述の命令のフォーマットは一つの例であり、他のフォーマットを用いても良い。

【００４２】以上のような処理をセキュアＤＦカードA-10内部で行わせることにより、端末A-20がセキュアＤＦカードのメモリに記録されたデータを外部に出力する際に、端末によりデータが不正に操作される懸念が払拭される。そのため、このセキュアＤＦカードを携帯電話やデジタルテレビのリモコンなどに装着し、セキュアＤＦカードのメモリに電子マネーやクレジットカード番号、個人情報など、秘匿を要するデータを格納して、携帯電話やテレビの画面を見ながらインターネットで電子商取引を行うことなどが可能になる。

【００４３】もし、カード自体がこのような処理を行わず、端末でデータを不正操作する可能性が残されている場合には、端末に対して、そうした不正が行われないような保証が求められることになる。これは、端末の機能を複雑化し、コストの上昇を余儀なくさせる。しかし、このセキュアＤＦカードを使用することにより、端末は、そのような責務から免れることができる。

【００４４】図7は、そうした一例として、携帯端末A-20に装着したセキュアＤＦカードA-10内のクレジットカード情報により、購入商品の決済を行う場合の処理手順を示している。まず、店舗で商品を購入したユーザが、店舗から決済要求を受ける（１）。ユーザは、携帯端末A-20から所有カード確認の操作を行う（２）。これを受けて端末の命令発行手段A-21から、セキュアＤＦカードA-10の命令実行手段A-11に対して所有カード情報確認命令が出される（３）。命令実行手段A-11は、記憶制御手段A-12に対して全ての所有カード情報を読み出すように命令を出し（４）、記憶手段A-13から読み出された全所有カード情報が命令実行手段A-11を通じて端末の命令発行手段A-21に送られ（５）、端末A-20の画面に表示される（６）。

【００４５】画面を見たユーザは、所有カードの中から使用カードを決定し（７）、使用カード指定操作を行う（８）。これを受けて端末の命令発行手段A-21は、セキュアＤＦカードA-10の命令実行手段A-11に使用カード番号の出力命令を出す（９）。命令実行手段A-11は、記憶

制御手段A-12に対して、指定された使用カード番号を読み出すように命令し、記憶手段A-13から読み出された使用カード番号を取得すると（１０）、外部通信制御手段A-14に、その使用カード番号の出力を命令する（１１）。外部通信制御手段A-14は、その命令に従って外部通信インタフェースA-16から使用カード番号を店舗に送信する（１２）。店舗では、そのカードの有効性を確認し（１３）、決済を実行して決済終了通知を発行する（１４）。

【００４６】このように、このセキュアＤＦカードA-10は、記憶手段A-13内部に持つデータを外部通信インタフェースA-16を介して外部に出力する場合、端末A-20を仲介せずに、それを行うことができる。

【００４７】なお、この実施形態では、端末の命令発行とカード内部動作とをシームレスに行う場合を示しているが、命令発行とカード内部動作とを時間差を置いて実現することとしても良い。これにより、例えば、接触／非接触両方のインタフェースを持つＩＣカードにおいて、携帯電話で接触インタフェースから電子マネー出力命令を発行し、そのＩＣカードを取り外して持ち歩き、非接触インタフェースを持つ支払機に対して決済処理を行う、と言う処理が可能になる。さらに、このＩＣカードは、支払機に対しては、あらかじめ受けていた命令である支払い処理しかできないようにする、と言う制限を掛けることも可能である。

【００４８】（第２の実施形態）第２の実施形態では、セキュアＤＦカードA-10が端末A-20から＜カード制御命令２＞を受信するまでと、受信した際の動作について、詳細を説明する。図１０に、本実施形態における＜命令２＞及び＜応答２＞、さらにその他の送受信データの構造をそれぞれ、（Ａ）～（Ｇ）として示す。

【００４９】図１０（Ａ）はセキュアＤＦカードA-10外部から、外部通信インタフェースA-16が受信する＜受信データ１＞を表している。G-01はヘッダにあたり、各々の受信データごとに、毎回異なる。受信データ長G-02は＜受信データ１＞の長さを示している。データ本体G-03は、記憶手段A-13に格納したいデータの本体を示す。終了識別子G-04は、＜受信データ１＞が終了することを示す識別子である。

【００５０】図１０（Ｂ）は、外部通信制御手段A-14が発行する＜データ受信通知１＞を表している。G-11は命令識別子C-01に対応し、＜データ受信通知１＞では“00100111”となる。メッセージ長G-12は命令長C-02に対応し、＜データ受信通知１＞の長さを示す。データG-13は命令内容C-03に対応し、＜受信データ１＞におけるデータ本体G-03となる。G-14は命令終了識別子C-04に対応し、＜データ受信通知１＞では“10100111”となる。

【００５１】図１０（Ｃ）は、命令実行手段A-11が発行する＜データ受信通知２＞を表している。G-21は命令識別子C-01に対応し、＜データ受信通知２＞では“00101000”となる。メッセージ長G-22は命令長C-02に対応し、＜データ受信通知２＞の長さを示す。インデックスG-23・データ本体長G-24は命令内容C-03に対応している。インデックスG-23は、＜受信データ１＞におけるデータ本体G-03から生成したインデックスデータである。データ本体長G-24は、＜受信データ１＞におけるデータ本体G-03の長さを示す。G-25は命令終了識別子C-04に対応し、＜データ受信通知２＞では“10101000”となる。

【００５２】図１０（Ｄ）は、命令発行手段A-21が発行する＜カード制御命令２＞を表している。G-31は命令識別子C-01に対応し、＜カード制御命令２＞では“00100001”となる。G-32は命令長C-02に対応し、＜カード制御命令２＞の長さを示す。先頭アドレスG-33・データ長G-34は命令内容C-03に対応している。先頭アドレスG-33は、＜カード制御命令２＞により記憶手段A-13内部に保存される、データ本体G-04の格納位置の先頭アドレス（論理アドレス）を示す。データ長G-34は、データ本体G-04を格納するために、記憶手段A-13内に確保する領域の大きさを示す。G-35は命令終了識別子C-04に対応し、＜カード制御命令２＞では“10100001”となる。

【００５３】図１０（Ｅ）は、命令実行手段A-11が発行する＜カード制御応答２＞を表している。G-41は応答識別子C-11に対応し、＜カード制御応答２＞では“00100010”となる。G-42は応答長C-12に対応し、＜カード制御応答２＞の長さを示す。処理結果G-43は応答内容C-13に対応し、＜カード制御命令２＞の実行結果の成功（“00000000”）または失敗（“11111111”）を示す数列が入る。G-44は応答終了識別子C-14に対応し、＜カード制御応答２＞では“10100010”となる。

【００５４】図１０（Ｆ）は、命令実行手段A-11が発行する＜記憶制御命令２＞を表している。G-51は命令識別子C-01に対応し、＜記憶制御命令２＞では“00100011”となる。G-52は命令長C-02に対応し、＜記憶制御命令２＞の長さを示す。先頭アドレスG-53・データ長G-54は命令内容C-03に対応している。先頭アドレスG-53は、＜記憶制御命令２＞により記憶手段A-13内部に保存される、データ本体G-04の格納位置の先頭アドレス（論理アドレス）を示す。データ長G-54は、データ本体G-04を格納するために、記憶手段A-13内に確保する領域の大きさを示す。G-55は命令終了識別子C-04に対応し、＜記憶制御命令２＞では“10100011”となる。

【００５５】図１０（Ｇ）は、記憶制御手段A-12が発行する＜記憶制御応答２＞を表している。G-61は応答識別子C-11に対応し、＜記憶制御応答２＞では“00100100”となる。G-62は応答長C-12に対応し、＜記憶制御応答２＞の長さを示す。処理結果G-63は応答内容C-13に対応し、＜記憶制御命令２＞の実行結果の成功（“00000000”）または失敗（“11111111”）を示す数列が入る。G-64は応答終了識別子C-14に対応し、＜記憶制御応答２＞では“10100100”となる。

【００５６】次に、セキュアＤＦカードA-10内部での動作について説明する。図８は、外部から入力されたデータをセキュアＤＦカード10のメモリ13に格納する場合のデータの流れ（①、②、⑤）と、端末20を通じてユーザの指示を待つ流れ（③、④）とをセキュアＤＦカードのハード構成上に簡略化して示している。

【００５７】図９は、この手順を詳細に示しており、図９において、矢印と括弧で囲んだ数字は、セキュアＤＦカードA-10が端末A-20から＜カード制御命令２＞を受信するまで、及び受信後の処理手順を模式的に示している。

（E-01）：外部通信制御手段A-14が、セキュアＤＦカードA-10外部から＜受信データ１＞を受信する。

（E-02）：＜受信データ１＞を受信した外部通信制御手段A-14は、＜受信データ１＞の解釈を行う（ここでは、ヘッダG-01の確認、G-02の部分から＜受信データ１＞の長さの確認、データ本体G-03の読み取り、終了識別子G-04の確認、を行う）。次に外部通信制御手段A-14は、＜データ受信通知１＞を生成し、命令実行手段A-11に送信する。

【００５８】（E-03）：＜データ受信通知１＞を受信した命令実行手段A-11は、＜データ受信通知１＞の解釈を行う（ここでは、G-11の部分が“00100111”であることの確認、G-12の部分から＜データ受信通知１＞の長さの確認、データG-13の読み取り、G-14の部分が“10100111”であることの確認、を行う）。次に命令実行手段A-11は、データ本体G-03から、データの内容を表す内容提示データとしてインデックスG-23を生成し、それを基に＜データ受信通知２＞を生成し、端末A-20に送信する。なお、インデックスG-23の生成は、例えば、データ本体G-03の一部を抽出することにより行う。

【００５９】（E-04）：＜データ受信通知２＞を受信した命令発行手段A-21は、＜データ受信通知２＞の解釈を行う（ここでは、G-21の部分が“00101000”であることの確認、G-22の部分から＜データ受信通知２＞の長さの確認、インデックスG-23・データ本体長G-24の読み取り、G-25の部分が“10101000”であることの確認、を行う）。次に端末A-20は、インデックスG-23を端末A-20やセキュアＤＦカードA-10のユーザに対して表示し、ユーザによる次の操作（受信データの記憶手段A-13への格納の可否）の待ち状態に入る。

【００６０】（E-05）：ユーザから次の操作（受信データの記憶手段A-13への格納可）を受けた端末A-20では、命令発行手段A-21が＜カード制御命令２＞を発行し、セキュアＤＦカードA-10に送信する。

（E-06）：＜カード制御命令２＞を受信した命令実行手段A-11は、＜カード制御命令２＞の解釈を行う（ここでは、G-31の部分が“00100001”であることの確認、G-32の部分から＜カード制御命令２＞の長さの確認、先頭アドレスG-33・データ長G-34の読み取り、G-35の部分が“10100001”であることの確認、を行う）。次に命令実行手段A-11は、外部通信制御手段A-14から受け取ったデータ本体G-03から＜記憶制御命令２＞を生成し、記憶制御手段A-12に送信する。このとき、命令実行手段A-11は、データ本体G-03を暗号化しても良い。

【００６１】（E-07）：＜記憶制御命令２＞を受信した記憶制御手段A-12は、＜記憶制御命令２＞の解釈を行う（ここでは、G-51の部分が“00100011”であることの確認、G-52の部分から＜記憶制御命令２＞の長さの確認、先頭アドレスG-53・データ長G-54・データ本体G-55の読み取り、G-56の部分が“10100011”であることの確認、を行う）。次に記憶制御手段A-12は、記憶手段A-13内に、先頭アドレスG-53からデータ長G-54の長さの領域を確保し、データ本体G-55を格納する。

【００６２】（E-08）：記憶制御手段A-12は、＜記憶制御応答２＞を生成し、命令実行手段A-11に送信する。

（E-09）：＜記憶制御応答２＞を受信した命令実行手段A-11は、＜記憶制御応答２＞の解釈を行う（ここでは、G-61の部分が“00100100”であることの確認、G-62の部分から＜記憶制御応答２＞の長さの確認、処理結果G-63の読み取り、G-64の部分が“10100100”であることの確認、を行う）。次に命令実行手段A-11は、＜記憶制御応答２＞内に含まれる、処理結果G-63に基づき、＜カード制御応答２＞を生成し、端末A-20に送信することで、＜カード制御命令２＞の処理結果を端末A-20に対して通知する。

【００６３】（E-10）：＜カード制御応答２＞を受信した命令発行手段A-21は、＜カード制御応答２＞の解釈を行う（ここでは、G-41の部分が“00100010”であることの確認、G-42の部分から＜カード制御応答２＞の長さの確認、処理結果G-43の読み取り、G-44の部分が“10100010”であることの確認、を行う）。

【００６４】この場合、命令実行手段A-11は、端末が出力する一つの＜カード制御命令２＞に対応する動作として、データ本体G-03からインデックスG-23を生成し＜データ受信通知２＞を生成して端末A-20に提示する動作と、＜記憶制御命令２＞を生成して記憶手段にデータを格納する動作との二つを行う。なお、前述の命令のフォーマットは一つの例であり、他のフォーマットを用いても良い。

【００６５】以上のような処理をセキュアＤＦカードA-10内部で行わせることにより、外部通信インタフェースA-16からデータを受信したとき、端末A-20にはそのインデックスだけを伝え、ユーザの意志を確認した上で、記憶手段A-13内部にデータが格納される。従って、外部通信インタフェースA-16から受信したデータを、端末A-20を仲介せずに記憶手段A-13内部に格納することが可能になる。

【００６６】例えば、電子商取引の領収書データが外部通信インタフェースA-16を通じて電子商店から送られて

来ると、命令実行手段A-11は、そのデータの2行目までのデータである“○×店領収書　２００２年１月１日”を抽出して端末に送る。これを端末の画面上で確認したユーザが領収書の保存を指示すると、命令実行手段A-11は、外部から送られた領収書データを記憶手段A-13に格納する。また、ユーザが、領収書の保存を不要とした場合には領収書データを廃棄する。この場合、端末には、領収書データそのものは送られないため、ユーザが領収書を改竄して保持すると言った不正を未然に防止することができる。

【００６７】なお、この実施形態においては、端末の命令発行とカード内部動作とはシームレスに行われることとしているが、命令発行とカード内部動作とを時間差を置いて実現することとしても良い。これにより、例えば、接触／非接触両面のインタフェースを持つＩＣカードにおいて、携帯電話で接触インタフェースから電子マネー充填命令を発行し、そのＩＣカードを取り外して持ち歩き、非接触インタフェースを持つ電子マネー充填機で充填処理を行う、などの処理が可能になる。さらに、このＩＣカードは、充填機に対しては、あらかじめ受けていた命令である充填処理しかできないようにする、と言う制限をかけることも可能となる。

【００６８】また、この実施形態においては、外部からの入力データを記憶手段に格納する場合についてのみ述べているが、命令実行手段が、入力データと記憶手段の別データとの照合を取り、その結果だけを端末に送信する、とする形態もある。これにより、例えば、携帯電話との接触インタフェースとＣＣＤカメラへのインタフェースとの両方を持つメモリカードにおいて、命令実行手段が、ＣＣＤカメラインタフェースから入力した画像データについて、記憶手段に保持されている正規の画像データと照合し、その判定結果のみを接触インタフェースから携帯電話上に表示する、と言ったことが可能になる。

【００６９】（第３の実施形態）第３の実施形態では、セキュアＤＦカードA-10が端末A-20から＜カード制御命令３＞を受信するまでと、受信した際の動作について、詳細を説明する。

【００７０】図１３に、本実施形態における＜命令３＞及び＜応答３＞、さらにその他の送受信データの構造をそれぞれ、（Ａ）～（Ｉ）として示す。図１３（Ａ）は、セキュアＤＦカードA-10外部から、外部通信インタフェースA-16が受信する＜受信データ２＞を表している。J-01はヘッダにあたり、各々の受信データごとに、毎回異なる。受信データ長J-02は＜受信データ２＞の長さを示している。出力要求J-03は、セキュアＤＦカードA-10が持つデータのうちの、どのデータを出力したいかを示している。終了識別子J-04は、＜受信データ２＞が終了することを示す識別子である。

【００７１】図１３（Ｂ）は、外部通信制御手段A-14が発行する＜データ受信通知３＞を表している。J-11は命令識別子C-01に対応し、＜データ受信通知３＞では“01000111”となる。メッセージ長J-12は命令長C-02に対応し、＜データ受信通知３＞の長さを示す。データJ-13は命令内容C-03に対応し、＜受信データ２＞における出力要求J-03と同様である。J-14は命令終了識別子C-04に対応し、＜データ受信通知３＞では“11000111”となる。

【００７２】図１３（Ｃ）は、命令実行手段A-11が発行する＜データ受信通知４＞を表している。J-21は命令識別子C-01に対応し、＜データ受信通知４＞では“01001000”となる。メッセージ長J-22は命令長C-02に対応し、＜データ受信通知４＞の長さを示す。インデックスJ-23・データ長J-24は命令内容C-03に対応している。インデックスJ-23は、出力要求J-03に基づき、＜記憶制御命令３＞＜記憶制御応答３＞により記憶手段A-13から取り出したデータについて、命令実行手段A-11が生成したインデックスデータである。データ長J-24は、＜記憶制御命令３＞＜記憶制御応答３＞により記憶手段A-13から取り出した、データの長さを示す。J-25は命令終了識別子C-04に対応し、＜データ受信通知４＞では“11001000”となる。

【００７３】図１３（Ｄ）は、命令発行手段A-21が発行する＜カード制御命令３＞を表している。J-31は命令識別子C-01に対応し、＜カード制御命令３＞では“01000001”となる。J-32は命令長C-02に対応し、＜カード制御命令３＞の長さを示す。データ長J-33は命令内容C-03に対応し、記憶手段A-13から外部に出力するデータの長さを示す。J-34は命令終了識別子C-04に対応し、＜カード制御命令３＞では“11000001”となる。

【００７４】図１３（Ｅ）は、命令実行手段A-11が発行する＜カード制御応答３＞を表している。J-41は応答識別子C-11に対応し、＜カード制御応答３＞では“01000010”となる。J-42は応答長C-12に対応し、＜カード制御応答３＞の長さを示す。処理結果J-43は応答内容C-13に対応し、＜カード制御命令３＞の実行結果の成功（“00000000”）または失敗（“11111111”）を示す数列が入る。J-44は応答終了識別子C-14に対応し、＜カード制御応答３＞では“11000010”となる。

【００７５】図１３（Ｆ）は、命令実行手段A-11が発行する＜記憶制御命令２＞を表している。G-51は命令識別子C-01に対応し、＜記憶制御命令３＞では“01000011”となる。J-52は命令長C-02に対応し、＜記憶制御命令３＞の長さを示す。先頭アドレスJ-53・データ長J-54は命令内容C-03に対応している。先頭アドレスJ-53は、記憶手段A-13内部に保持されている、出力要求J-03で指定されたデータの先頭アドレス（論理アドレス）を示す。データ長J-54は、記憶手段A-13内部に保持されている、出力要求J-03で指定されたデータの長さを示す。J-55は命令終了識別子C-04に対応し、＜記憶制御命令３＞では“11000011”となる。

【００７６】図１３（Ｇ）は、記憶制御手段A-12が発行する＜記憶制御応答３＞を表している。J-61は応答識別子C-11に対応し、＜記憶制御応答３＞では“01000100”となる。J-62は応答長C-12に対応し、＜記憶制御応答３＞の長さを示す。データ長J-63・データ本体J-64は応答内容C-13に対応している。データ長J-63は、後に続くデータ本体J-64の長さを示す。データ本体J-64は、＜記憶制御命令３＞により指定され、記憶手段A-13から取り出されたデータの本体が入る。J-64は応答終了識別子C-14に対応し、＜記憶制御応答３＞では“11000100”となる。

【００７７】図１３（Ｈ）は、命令実行手段A-11が発行する＜通信制御命令３＞を表している。J-71は命令識別子C-01に対応し、＜通信制御命令３＞では“01000101”となる。J-72は命令長C-02に対応し、＜通信制御命令３＞の長さを示す。データ長J-73・データ本体J-74は命令内容C-03に対応している。データ長J-73・データ本体J-74が持つ意味は、＜記憶制御応答３＞におけるデータ長J-63・データ本体J-64と同様である。J-75は命令終了識別子C-04に対応し、＜通信制御命令３＞では“11000101”となる。

【００７８】図１３（Ｉ）は、外部通信制御手段A-14が発行する＜通信制御応答３＞を表している。J-81は応答識別子C-11に対応し、＜通信制御応答３＞では“01000110”となる。J-82は応答長C-12に対応し、＜通信制御応答３＞の長さを示す。処理結果J-83は応答内容C-13に対応し、＜通信制御命令３＞の実行結果の成功（“00000000”）または失敗（“11111111”）を示す数列が入る。J-84は応答終了識別子C-14に対応し、＜通信制御応答３＞では“11000110”となる。

【００７９】次に、セキュアＤＦカードA-10内部での動作について説明する。図１１は、外部からの要求を受け、ユーザの意志を確認した後、セキュアＤＦカード10のメモリ13で保持されたデータを外部に出力する場合のメモリ13への指示の流れ（①～③）と、端末の指示を待つ流れ（⑤～⑥）と、メモリ13から読み出されたデータの流れ（④、⑦～⑧）とをセキュアＤＦカードのハード構成上に簡略化して示している。

【００８０】図１２は、この手順を詳細に示しており、図１２において、矢印と括弧で囲んだ数字は、セキュアＤＦカードA-10が端末A-20から＜カード制御命令３＞を受信するまで、及び受信後の処理手順を模式的に示している。

（H-01）：外部通信制御手段A-14が、セキュアＤＦカードA-10外部から＜受信データ２＞を受信する。

（H-02）：＜受信データ２＞を受信した外部通信制御手段A-14は、＜受信データ２＞の解釈を行う（ここでは、ヘッダJ-01の確認、J-02の部分から＜受信データ２＞の長さの確認、出力要求J-03の読み取り、終了識別子J-04の確認、を行う）。次に外部通信制御手段A-14は、＜データ受信通知３＞を生成し、命令実行手段A-11に送信する。

【００８１】（H-03）：＜データ受信通知３＞を受信した命令実行手段A-11は、＜データ受信通知３＞の解釈を行う（ここでは、J-11の部分が“01000111”であることの確認、J-12の部分から＜データ受信通知３＞の長さの確認、データJ-13の読み取り、J-14の部分が“11000111”であることの確認、を行う）。次に命令実行手段A-11は、＜記憶制御命令３＞を生成し、記憶制御手段A-12に送信する。

（H-04・H-05）：＜記憶制御命令３＞を受信した記憶制御手段A-12は、＜記憶制御命令３＞の解釈を行う（ここでは、J-51の部分が“01000011”であることの確認、J-52の部分から＜記憶制御命令３＞の長さの確認、先頭アドレスJ-53・データ長J-54の読み取り、J-55の部分が“11000011”であることの確認、を行う）。次に記憶制御手段A-12は、＜記憶制御命令３＞に記された先頭アドレスJ-53とデータ長J-54とから、指定されたデータを記憶手段A-13から取り出す。

【００８２】（H-06）：記憶制御手段A-12は、記憶手段A-13から取り出したデータから＜記憶制御応答３＞を生成し、命令実行手段A-11に送信する。

（H-07）：＜記憶制御応答３＞を受信した命令実行手段A-11は、＜記憶制御応答３＞の解釈を行う（ここでは、J-61の部分が“01000100”であることの確認、J-62の部分から＜記憶制御応答３＞の長さの確認、データ長J-63・データ本体J-64の読み取り、D-35の部分が“11000100”であることの確認、を行う）。次に命令実行手段A-11は、データ本体J-64から、データの内容を表す内容提示データとしてインデックスJ-23を生成する。

【００８３】（H-08）：次に命令実行手段A-11は、データ長J-63とインデックスJ-23とから＜データ受信通知４＞を生成し、端末A-20に対して送信する。

（H-09）：＜データ受信通知４＞を受信した命令発行手段A-21は、＜データ受信通知４＞の解釈を行う（ここでは、J-21の部分が“01001000”であることの確認、J-22の部分から＜データ受信通知４＞の長さの確認、インデックスJ-23・データ長J-24の読み取り、J-25の部分が“11001000”であることの確認、を行う）。次に端末A-20は、インデックスG-23を端末A-20やセキュアＤＦカードA-10のユーザに対して表示し、ユーザによる次の操作（該当データの記憶手段A-13から外部への出力の可否）の待ち状態に入る。

【００８４】（H-10）：ユーザから次の操作（該当データの記憶手段A-13から外部への出力可）を受けた端末A-20では、命令発行手段A-21が＜カード制御命令３＞を発行し、セキュアＤＦカードA-10に送信する。

（H-11）：＜カード制御命令３＞を受信した命令実行手段A-11は、＜カード制御命令３＞の解釈を行う（ここでは、J-31の部分が“01000001”であることの確認、J-32

の部分から<カード制御命令３>の長さの確認、データ長J-33の読み取り、J-34の部分が“11000001”であることの確認、を行う）。次に命令実行手段A-11は、データ長J-33・データ本体J-64から<通信制御命令３>を生成し、外部通信制御手段A-14に送信する。なお、このとき命令実行手段A-11は、データ本体を暗号化して<通信制御命令３>に含めるようにしても良い。

【００８５】（H-12）：<通信制御命令３>を受信した外部通信制御手段A-14は、<通信制御命令３>の解釈を行う（ここでは、J-71の部分が“01000101”であることの確認、J-72の部分から<通信制御命令３>の長さの確認、データ長J-73・データ本体J-74の読み取り、J-75の部分が“11000101”であることの確認、を行う）。次に外部通信制御手段A-14は、<通信制御命令３>内に含まれる、データ本体J-74を、外部通信インタフェースA-16からセキュアＤＦカードA-10の外部に出力する。

（H-13）：目的のデータの外部への出力が終了すると、外部通信制御手段A-14は<通信制御応答３>を生成し、命令実行手段A-11に送信する。

【００８６】（H-14）：<通信制御応答３>を受信した命令実行手段A-11は、<通信制御応答３>の解釈を行う（ここでは、J-81の部分が“01000110”であることの確認、J-82の部分から<通信制御応答３>の長さの確認、処理結果J-83の読み取り、J-84の部分が“11000110”であることの確認、を行う）。次に命令実行手段A-11は、<通信制御応答３>内に含まれる、処理結果J-83に基づき、<カード制御応答３>を生成し、端末A-20に送信することで、<カード制御命令３>の処理結果を端末A-20に対して通知する。

【００８７】（H-15）：<カード制御応答３>を受信した命令発行手段A-21は、<カード制御応答３>の解釈を行う（ここでは、J-41の部分が“01000010”であることの確認、J-42の部分から<カード制御応答３>の長さの確認、処理結果J-43の読み取り、J-44の部分が“11000010”であることの確認、を行う）。この処理結果J-43の内容を命令発行手段A-21が検証することにより、端末A-20は<カード制御命令３>の実行結果を確認する。

【００８８】この場合、命令実行手段A-11は、端末が出力する一つの<カード制御命令３>に対応する動作として、<記憶制御命令３>を生成して記憶手段からデータを読み出す動作と、データ本体J-64からインデックスJ-23を生成し<データ受信通知４>を生成して端末A-20に提示する動作と、<通信制御命令３>を生成して外部にデータを送信する動作との三つを行う。なお、前述の命令のフォーマットは一つの例であり、他のフォーマットを用いても良い。

【００８９】以上のような処理をセキュアＤＦカードA-10内部で行わせることにより、外部からの要求に基づき、記憶手段A-13内部に持つデータを、ユーザの意思確認を可能としながら、データそのものは端末A-20を介することなく、セキュアＤＦカードA-10外部に出力することが可能になる。

【００９０】例えば、このセキュアＤＦカードを、食堂のトレーに載せた皿の形状からカードの料金を引き去る食堂システムに適用した場合、外部通信インタフェースA-16から入力した料金請求に基づいて、端末にユーザの意思を確認する画面が表示され、ユーザが了承したときに請求金額に相当する電子マネーが外部通信インタフェースA-16から出力される。この場合、ユーザは、請求金額を見てトレーに載せた皿を減らす選択も可能になる。

【００９１】なお、各実施形態では、端末の命令に基づいて、端末を介さずに、記憶手段に格納したデータを外部通信インタフェースから出力したり、外部通信インタフェースから入力したデータを記憶手段に格納したりするセキュアＤＦカードの動作について説明したが、端末の命令が、記憶手段から読み出したデータを端末へ出力し、あるいは、端末から入力したデータを記憶手段に格納することを命じている場合には、その命令に従って、端末を介して、データの入出力を行うことが可能となる。つまり、命令実行手段が実行する命令の中に「端末を介さない」ことを意味する情報が有るか無いかにより、本カードでデータ入出力する際に、端末を介すか介さないかが決まり、その切替は、命令の記述によって制御できる。

【００９２】一方、カードの仕組みとして、記憶手段から読み出したデータ、または、記憶手段に書き込むデータは、全て端末を介さずに入出力される（つまり、命令の中で「端末を介す」か「介さない」かを区別しなくても、一律に端末を介さずにデータが入出力される）ように構成し、別の言い方をすれば、端末通信インタフェースを介したデータの入出力または端末通信インタフェースへの入出力が予定されているデータの記憶手段からの読み出し／書き込みは一切行わないこととし、端末には、せいぜい命令実行手段が生成したインデックスや書き込み時の確認用データのほか、情報提示を目的とするデータなど、記憶手段からの読み出し／書き込み対象となる実体データ以外の情報だけが送られるように構成することもできる。

【００９３】

【発明の効果】以上の説明から明らかなように、本発明のセキュアＤＦカードでは、カード内部のデータの出力に際し、端末の不正動作の可能性に対して、出力データの秘匿性・完全性の保持を実現する。

【００９４】また、カード・端末外部からのデータのカード内部への入力に際しても、端末の不正動作の可能性に対して、入力データの秘匿性・完全性の保持を実現する。また、カード・端末外部からのデータのカード内部への入力に際して、カード・端末ユーザに対し、データの妥当性の判断を促すことが可能になる。

【００９５】また、カード・端末以外の外部からのトリ

ガーによる、カード内部のデータの出力に際し、端末の不正動作の可能性に対して、出力データの秘匿性・完全性の保持を実現する。

【００９６】また、カード・端末以外の外部からのトリガーによる、カード内部のデータの出力に際して、カード・端末ユーザに対し、操作の妥当性の判断を促すことが可能になる。

【図面の簡単な説明】

【図１】本発明の実施形態におけるＤＦカードのハード構成図

【図２】本発明の実施形態におけるセキュアＤＦカード及び端末の構成図

【図３】本発明の実施形態における命令及び応答の基本フォーマットを示す図

【図４】本発明の第１の実施形態における各命令及び応答の内容を示す図

【図５】本発明の第１の実施形態におけるセキュアＤＦカードの内部データの出力方法の概略を示す図

【図６】本発明の第１の実施形態におけるセキュアＤＦカード内部データの出力方法を示す図

【図７】本発明の第１の実施形態におけるＤＦカードのクレジットカード情報を利用する場合の具体例

【図８】本発明の第２の実施形態におけるセキュアＤＦカードへの外部データの格納方法の概略を示す図

【図９】本発明の第２の実施形態におけるセキュアＤＦカードへの外部データの格納方法を示す図

【図１０】本発明の第２の実施形態における送受信データと各命令及び応答の内容を示す図

【図１１】本発明の第３の実施形態におけるセキュアＤＦカード内部データの出力方法の概略を示す図

【図１２】本発明の第３の実施形態におけるセキュアＤＦカード内部データの出力方法を示す図

【図１３】本発明の第３の実施形態における送受信データと各命令及び応答の内容を示す図

【図１４】従来技術例１～３のＤＦカードのハード構成図

【図１５】従来技術例１～３におけるＤＦカード及び端末の構成図

【図１６】従来技術例１におけるＤＦカード内部データの出力方法を示す図

【図１７】従来技術例１におけるＤＦカード内部データの出力方法の概略を示す図

【図１８】従来技術例２におけるＤＦカードへの外部データの格納方法を示す図

【図１９】従来技術例２におけるＤＦカードへの外部データの格納方法の概略を示す図

【図２０】従来技術例３におけるＤＦカード内部データの出力方法を示す図

【図２１】従来技術例３におけるＤＦカード内部データの出力方法の概略を示す図

【図２２】従来技術例４におけるＩＣカードと端末の構成及びカード内部データの読み出し方法を示す図

【符号の説明】

10　セキュアＤＦカード
11　ＤＦコントローラ
13　フラッシュメモリ
14　ＤＦＩＯコントローラ
20　端末
30　カード
31　メモリコントローラ
33　フラッシュメモリ
34　ＩＯコントローラ
A-10　セキュアＤＦカード
A-11　命令実行手段
A-12　記憶制御手段
A-13　記憶手段
A-14　外部通信制御手段
A-15　端末通信インタフェース
A-16　外部通信インタフェース
A-20　端末
A-21　命令発行手段
A-22　カード通信インタフェース
B-01～B-10　第１の実施形態における命令・応答・データ・処理のフロー
C-01　命令識別子
C-02　命令長
C-03　命令内容
C-04　命令終了識別子
C-11　応答識別子
C-12　応答長
C-13　応答内容
C-14　応答終了識別子
D-01　＜カード制御命令１＞の命令識別子
D-02　命令長
D-03　先頭アドレス
D-04　データ長
D-05　＜カード制御命令１＞の命令終了識別子
D-11　＜カード制御応答１＞の応答識別子
D-12　応答長
D-13　処理結果
D-14　＜カード制御応答１＞の応答終了識別子
D-21　＜記憶制御命令１＞の命令識別子
D-22　命令長
D-23　先頭アドレス
D-24　データ長
D-25　＜記憶制御命令１＞の命令終了識別子
D-31　＜記憶制御応答１＞の応答識別子
D-32　応答長
D-33　データ長
D-34　データ本体

27

D-35 <記憶制御応答1>の応答終了識別子
D-41 <通信制御命令1>の命令識別子
D-42 命令長
D-43 データ長
D-44 データ本体
D-45 <通信制御命令1>の命令終了識別子
D-51 <通信制御応答1>の応答識別子
D-52 応答長
D-53 処理結果
D-54 <通信制御応答1>の応答終了識別子
E-01～E-10 第2の実施形態における命令・応答・データ・処理のフロー
G-01 <受信データ1>のヘッダ
G-02 受信データ長
G-03 データ本体
G-04 <受信データ1>の終了識別子
G-11 <データ受信通知1>の識別子
G-12 メッセージ長
G-13 データ
G-14 <データ受信通知1>の終了識別子
G-21 <データ受信通知2>の識別子
G-22 メッセージ長
G-23 インデックス
G-24 データ本体長
G-25 <データ受信通知2>の終了識別子
G-31 <カード制御命令2>の命令識別子
G-32 命令長
G-33 先頭アドレス
G-34 データ長
G-35 <カード制御命令2>の命令終了識別子
G-41 <カード制御応答2>の応答識別子
G-42 応答長
G-43 処理結果
G-44 <カード制御応答2>の応答終了識別子
G-51 <記憶制御命令2>の命令識別子
G-52 命令長
G-53 先頭アドレス
G-54 データ長
G-55 データ本体
G-56 <記憶制御命令2>の命令終了識別子
G-61 <記憶制御応答2>の応答識別子
G-62 応答長
G-63 処理結果
G-64 <記憶制御応答2>の応答終了識別子
H-01～H-15 第3の実施形態における命令・応答・データ・処理のフロー
J-01 <受信データ2>のヘッダ
J-02 受信データ長
J-03 出力要求
J-04 <受信データ2>の終了識別子

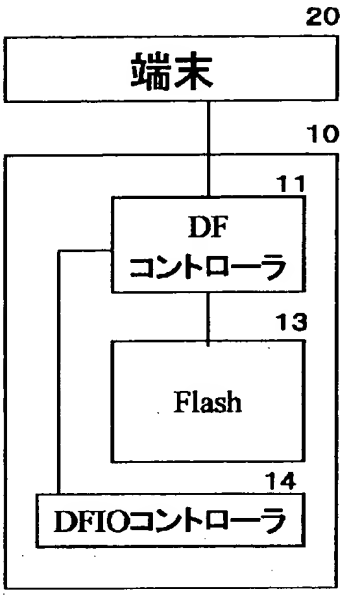
28

J-11 <データ受信通知3>の識別子
J-12 メッセージ長
J-13 データ
J-14 <データ受信通知3>の終了識別子
J-21 <データ受信通知4>の識別子
J-22 メッセージ長
J-23 インデックス
J-24 データ長
J-25 <データ受信通知4>の終了識別子
J-31 <カード制御命令3>の命令識別子
J-32 命令長
J-33 データ長
J-34 <カード制御命令3>の命令終了識別子
J-41 <カード制御応答3>の応答識別子
J-42 応答長
J-43 処理結果
J-44 <カード制御応答3>の応答終了識別子
J-51 <記憶制御命令3>の命令識別子
J-52 命令長
J-53 先頭アドレス
J-54 データ長
J-55 <記憶制御命令3>の命令終了識別子
J-61 <記憶制御応答3>の応答識別子
J-62 応答長
J-63 データ長
J-64 データ本体
J-65 <記憶制御応答3>の応答終了識別子
J-71 <通信制御命令3>の命令識別子
J-72 命令長
J-73 データ長
J-74 データ本体
J-75 <通信制御命令3>の命令終了識別子
J-81 <通信制御応答3>の応答識別子
J-82 応答長
J-83 処理結果
J-84 <通信制御応答3>の応答終了識別子
Z-11 命令実行手段
Z-12 記憶制御手段
Z-13 記憶手段
Z-14 外部通信制御手段
Z-15 端末通信インタフェース
Z-16 外部通信インタフェース
Z-21 命令発行手段
Z-22 カード通信インタフェース
Y-01～Y-05 従来技術例1における命令・応答・データ・処理のフロー
X-01～X-06 従来技術例2における命令・応答・データ・処理のフロー
W-01～W-06 従来技術例3における命令・応答・データ・処理のフロー

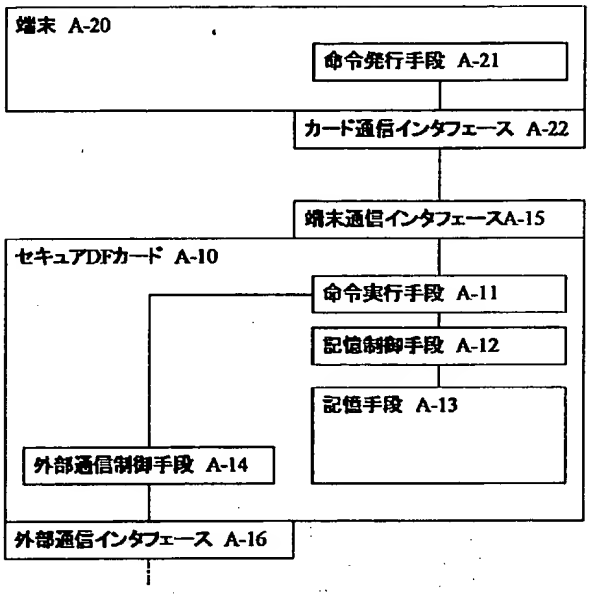
29　　30

V-01～V-04　従来技術例4における命令・応答・データ・処理のフロー
V-11　命令実行手段
V-12　記憶制御手段
V-13　記憶手段
V-14　端末通信インタフェース
V-21　命令発行手段
V-22　カード通信インタフェース

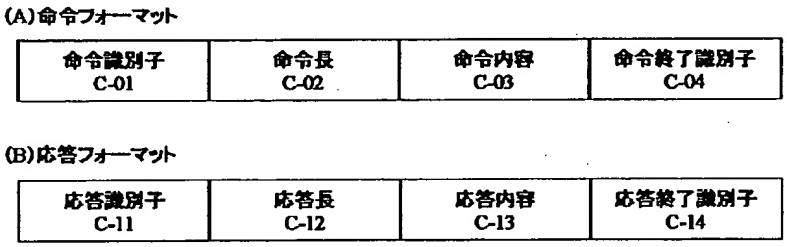
【図1】



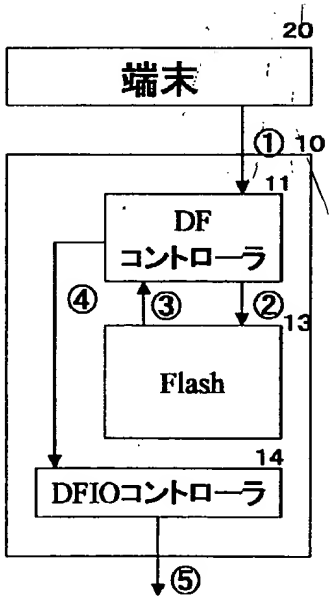
【図2】



【図3】



【図5】



【図4】

(A)<カード制御命令1>

00001001 D-01	命令長 D-02	先頭アドレス D-03	データ長 D-04	10001001 D-05

(B)<カード制御応答1>

00001010 D-11	応答長 D-12	処理結果 D-13	10001010 D-14

(C)<記憶制御命令1>

00001011 D-21	命令長 D-22	先頭アドレス D-23	データ長 D-24	10001011 D-25

(D)<記憶制御応答1>

00001100 D-31	応答長 D-32	データ長 D-33	データ本体 D-34	10001100 D-35

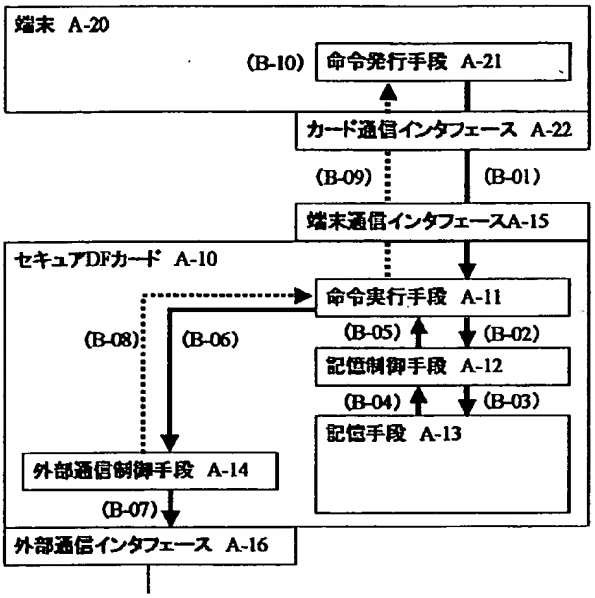
(E)<通信制御命令1>

00001101 D-41	命令長 D-42	データ長 D-43	データ本体 D-44	10001101 D-45

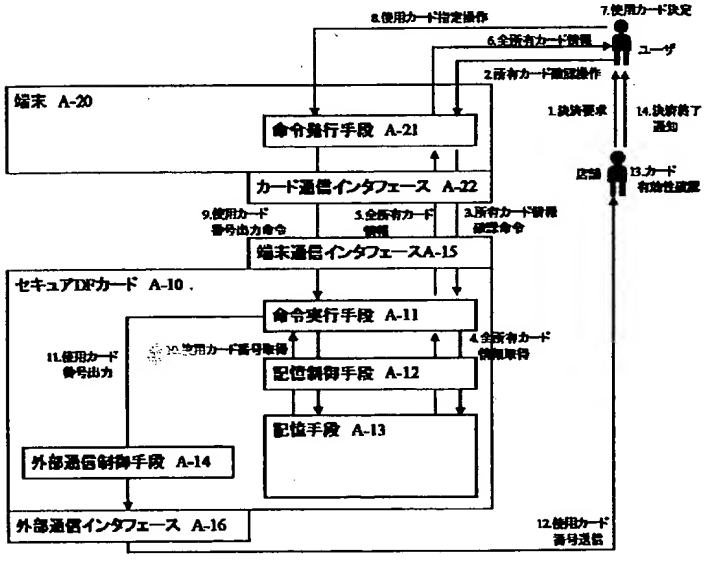
(F)<通信制御応答1>

00001110 D-51	応答長 D-52	処理結果 D-53	10001110 D-54

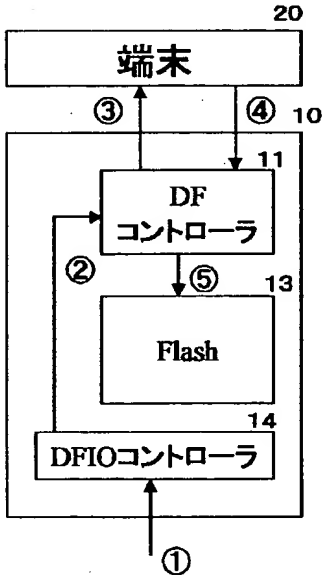
【図6】



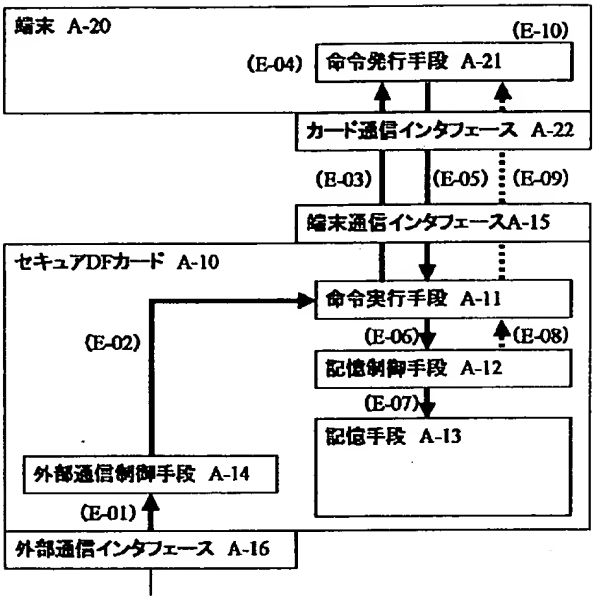
【図7】



【図8】



【図9】



【図10】

(A)<受信データ1>

ヘッダ G-01	受信データ長 G-02	データ本体 G-03	終了識別子 G-04

(B)<データ受信通知1>

00100111 G-11	メッセージ長 G-12	データ G-13	10100111 G-14

(C)<データ受信通知2>

00101000 G-21	メッセージ長 G-22	インデックス G-23	データ本体長 G-24	10101000 G-25

(D)<カード制御命令2>

00100001 G-31	命令長 G-32	先頭アドレス G-33	データ長 G-34	10100001 G-35

(E)<カード制御応答2>

00100010 G-41	応答長 G-42	処理結果 G-43	10100010 G-44

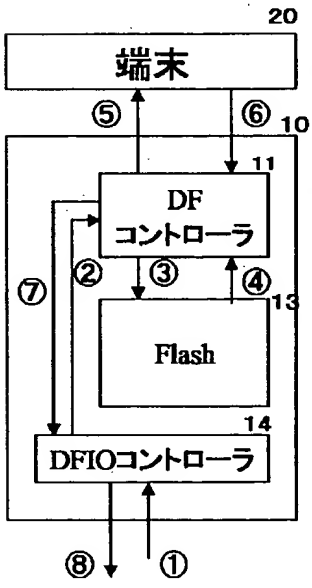
(F)<記憶制御命令2>

00100011 G-51	命令長 G-52	先頭アドレス G-53	データ長 G-54	データ本体 G-55	10100011 G-56

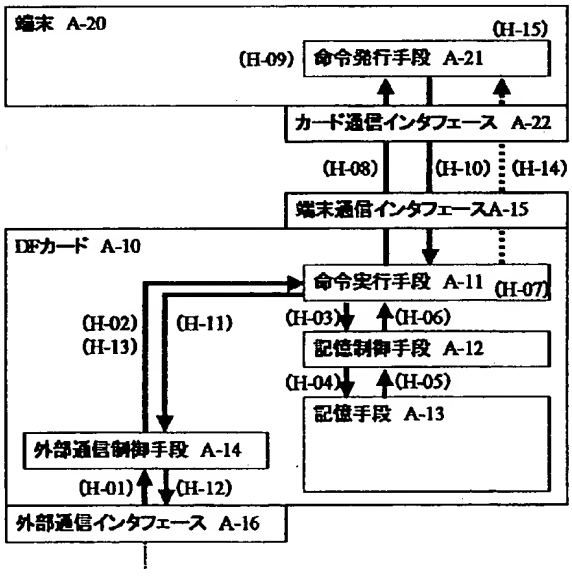
(G)<記憶制御応答2>

00100100 G-61	応答長 G-62	処理結果 G-63	10100100 G-64

【図11】

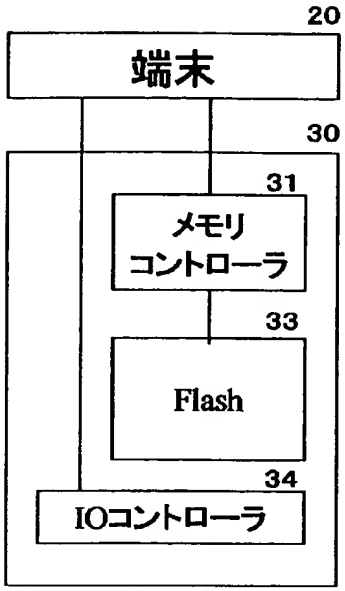


【図12】

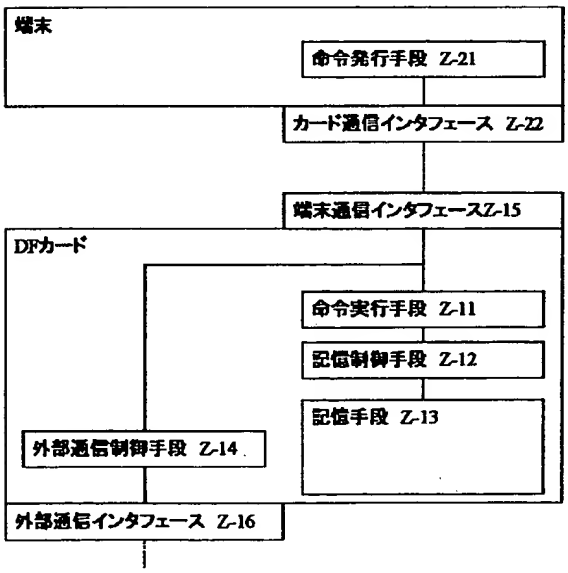


【図13】

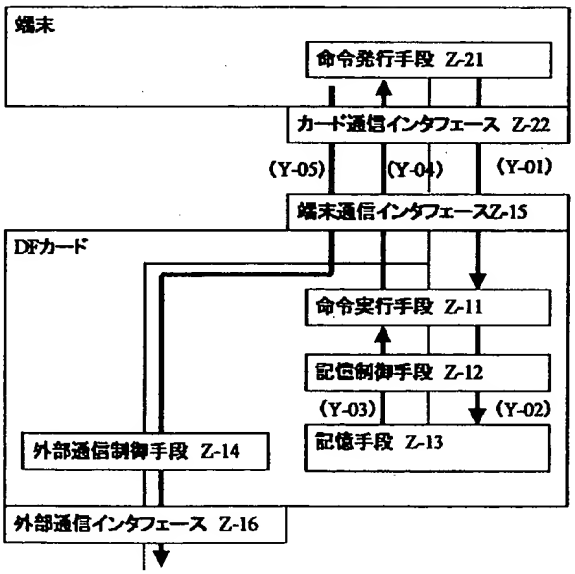
【図14】



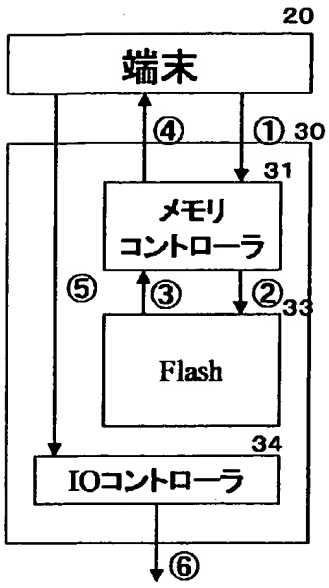
【図15】



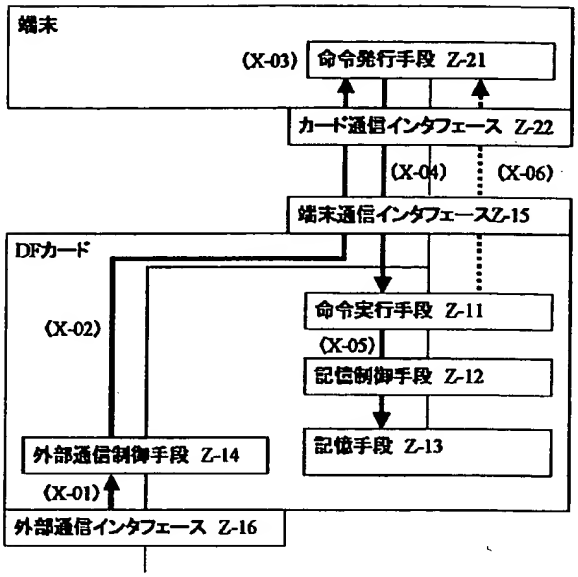
【図16】



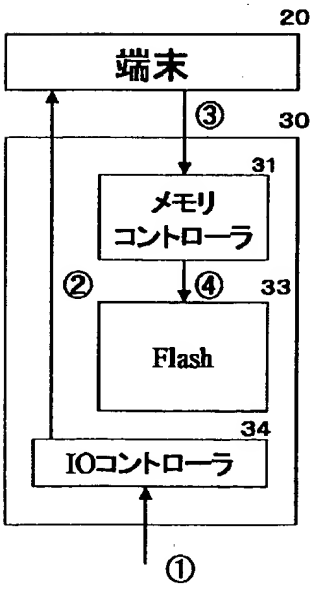
【図17】



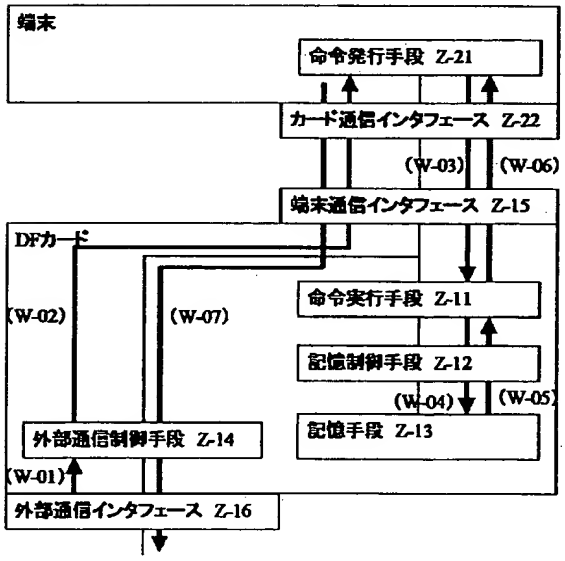
【図18】



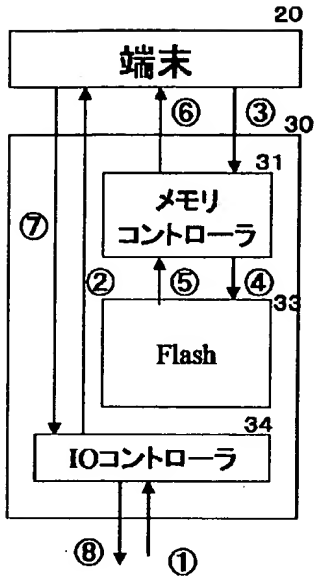
【図19】



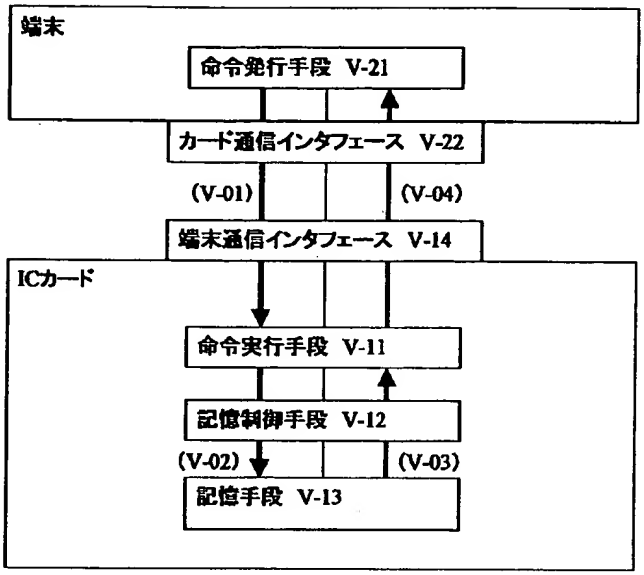
【図20】



【図21】



【図22】



フロントページの続き

(72)発明者　高木　佳彦
大阪府門真市大字門真1006番地　松下電器
産業株式会社内

Fターム(参考)　2C005 MA05 MB03 NA02 NA06 SA05
SA21 SA26
5B035 AA13 BB09 BC00 CA11 CA38
5B065 BA09 CA13 CC08